УДК 343.85

Топчій Віталій Васильович,
кандидат юридичних наук,
прокурор відділу прокуратури Київської області
(Прокуратура Київської області)

Тичина Дмитро Михайлович,
кандидат юридичних наук,
старший науковий співробітник
(Національна академія внутрішніх справ)

ЗАПОБІГАННЯ ВИКОРИСТАННЮ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗЛОЧИННИХ ЦІЛЯХ

У статті розглянуто проблемні питання комп'ютерної злочинності (кіберзлочинів); формування інформаційного простору, заснованого на використанні електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; захисту комп'ютерної інформації від несанкціонованого (незаконного) втручання; діючого законодавства у цій сфері; запобіжних заходів щодо забезпечення захисту інформаційного простору у державі.

Ключові слова: *комп'ютерні злочини; кіберзлочини; комп'ютерна злочинність; комп'ютерна інформація; інформаційний простір; електронно-обчислювальні машини (комп'ютери); комп'ютерні системи та мережі; мережі електрозв'язку; запобіжні заходи щодо забезпечення захисту інформаційного простору.*

Зміни соціального середовища держави, пов'язані з новим сплеском технічної еволюції, на сучасному етапі розвитку суспільства характеризуються наступними кримінологічно-значимими обставинами:

а) комп'ютеризація суспільства призвела до появи нових технологій учинення злочинів. Сьогодні багато традиційних злочинів неможливо здійснювати або масштабно, або без ризику швидкого викриття, якщо не використовувати високі технології. Тому магазини все частіше спустошуються через Інтернет за допомогою системи електронних платежів, а банківські сейфи — за допомогою неправомірного доступу в автоматизовані системи міжбанківських розрахунків;

б) формування інформаційного простору, заснованого на використанні електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також взаємопов'язаних із цим процесів зародження і розвитку суспільних відносин у сфері комп'ютерної інформації стали основою виникнення нових видів злочинної діяльності. Це стосується кримінального законодавства України у сфері комп'ютерної злочинності, де з'явилися такі злочини, як комп'ютерне піратство; виготовлення або збут підроблених кредитних або розрахункових карток; неправомірний доступ до охоронюваної законом комп'ютерної інформації; створення, поширення і використання шкідливих програм для ЕОМ; порушення правил експлуатації ЕОМ, систем ЕОМ або їхніх мереж та ін. [1];

в) повсюдне і всебічне впровадження нових технологій призводить до технічного оснащення окремих злочинців і організованих злочинних формувань. Високопрофесійні

фахівці, які працюють на таких злочинців, вже створили цілі комп'ютерні платформи систем ЕОМ та їхніх мереж.

Комп'ютерні злочини є новим видом суспільно небезпечних діянь, і визначення їм необхідно давати з урахуванням ознаки, яка є основою чинної класифікації злочинів. Саме поняття «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» («***комп'ютерні злочини»***) можна сформулювати як *суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку.* До таких злочинів слід відносити злочини, передбачені статтями 361 — 363-1 КК України [2].

Актуальність дослідження комп'ютерних злочинів, на думку Н. С. Козака, обумовлена тим, що особливості формулювання норм КК України щодо даних злочинів певною мірою ускладнюють, а в деяких випадках практично унеможливлюють їхнє застосування, зумовлюють неоднозначне їх розуміння працівниками правоохоронних і судових органів, що призводить до виникнення помилок при кваліфікації цих злочинів [3].

Проблеми комп'ютерних злочинів в Україні досліджували: Д. Азаров, П. Андрушко, Ю. Баулін, П. Біленчук, А. Білоусов, В. Бутузов, В. Гавловський, В. Голина, Б. Головкін, В. Голубєв, М. Гуцалюк, Ю. Заїка, М. Карчевський, М. Коваленко, Н. Козак, О. Користін, В. Кузнецов, Б. Кузьменко, С. Кузьмін, О. Литвинов, А. Музика, Д. Никифорчук, Ю. Орлов, С. Остапець, М. Плугатир, Н. Розенфельд, Б. Романюк, М. Рудик, А. Савченко, Г. Усатий, В. Хахановський, В. Цимбалюк, В. Шеломенцев, Я. Якубовський та ін.

Поява перших комп'ютерних злочинів і подальше зростання комп'ютерної злочинності були обумовлені переходом на автоматизовані системи документообігу. Так, перші розкрадання за допомогою незаконних маніпуляцій з комп'ютерною інформацією відбувалися під час переходу відділень зв'язку на нову централізовану автоматичну систему обробки (отримання і відправки) грошових переказів клієнтів, яка функціонувала на базі комп'ютерного комплексу «Онега». Разом із цією системою застосовувався звичайний ручний спосіб прийому і відправки платежів. Паралельне використання автоматизованих і неавтоматизованих операцій із грошовими коштами дозволило особам, які працювали у відділеннях зв'язку, здійснювати розкрадання [4, с. 16–18].

Процеси автоматизації банківської діяльності визначили якісно новий етап зростання комп'ютерної злочинності. Період з 1991 по 1997 рік був найбільш вигідним для здійснення комп'ютерних злочинів. Цей час відрізнявся вкрай привабливими для скоєння комп'ютерних злочинів умовами. Аналіз даного періоду дозволяє виділити основні причини зростання комп'ютерної злочинності.

По-перше, на початку 90-х років XX ст. практично не було прийнято законодавства, що регулює інформаційні правопорушення. Більше того, КК України 1960 р. [5] не передбачав адекватної кримінальної відповідальності за комп'ютерні злочини. Відсутність відповідного кримінально-правового захисту змушувало правоохоронні органи або не помічати, або використовувати абсолютно неприйнятні методи боротьби з комп'ютерною злочинністю.

По-друге, більшість організацій не здійснювало достатніх заходів щодо забезпечення безпеки експлуатованих ЕОМ, систем ЕОМ, мереж ЕОМ. Фахівці з інформаційної безпеки відзначали явне небажання багатьох керівників проводити роботу і вживати заходів щодо захисту автоматизованих систем від неправомірного доступу. Як правило, відмова пояснювалася небажаними додатковими обмеженнями для користувачів і суттєвими матеріальними витратами.

По-третє, у правоохоронних органах не було спеціальних підрозділів, що здійснюють боротьбу з комп'ютерною злочинністю, не вистачало кваліфікованих працівників через

низьку оплату праці. І це помітно знижувало активність звернення потерпілих від комп'ютерних злочинів за допомогою до правоохоронних органів.

Сприятливі умови для здійснення комп'ютерних злочинів та соціальна ситуація того періоду характеризуються активними ринковими перетвореннями і масовим зубожінням більшої частини населення країни, що визначили причини й умови (детермінанти) вчинення цих суспільно небезпечних діянь, які втілюються в мотивації злочинців.

Більшість комп'ютерних злочинів учинялися з метою збагачення. Із усієї кількості зареєстрованих і проаналізованих злочинів 52 % було пов'язано з розкраданнями коштів, 16 % — із руйнуванням і знищенням програмного забезпечення комп'ютерної техніки, 12 % — із навмисним перекручуванням вихідних даних, 10 % — із розкраданням інформації та програм, 10 % — із розкраданням послуг [6].

Починаючи з 2000-х років збільшується кількість досліджень комп'ютерних злочинів (або кіберзлочинності) [7; 8; 9; 10; 11; 12, с. 293–303], публікацій про різні аспекти кримінально-правової характеристики, кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що передбачені статтями 361–363[1] КК України, а також про так званий «кібертероризм» — явище, яке характеризується тим, що комп'ютерні злочини стають елементами системної терористичної діяльності [13; 14; 15]. Ученими дається кримінально-правова характеристика комп'ютерних злочинів та коментуються питання щодо кваліфікації даних злочинів [16; 17; 18]. Вносяться відповідні зміни до законодавства, зокрема до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-вр (за станом на 19 квітня 2014 р.) [19] та Кодексу України про адміністративні правопорушення (за станом на 11 червня 2017 р.) [20].

Даний період характеризується процесами створення державою сприятливих умов для розвитку сфери комп'ютерної інформації. Зокрема, уведено кримінальну відповідальність за злочини в цій сфері, що передбачені у розділі XVI «Злочини» у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (ст. 361–363-[1]) КК України [1]:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України);

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-[1] КК України);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-[2] КК України);

– несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України);

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-[1] КК України) [1].

Надалі комп'ютерні злочини віднесено до альтернативної підслідності СБУ і МВС. Для здійснення боротьби з комп'ютерною злочинністю у правоохоронних органах створені спеціальні підрозділи.

У цілому ж представлені вище проблеми боротьби з комп'ютерною злочинністю (відсутність інформаційного законодавства, нечисленність кваліфікованих кадрів у правоо-

хоронних органах, проблеми кваліфікації комп'ютерних злочинів та ін.) залишилися не розглянутими та повинні бути враховані під час здійснення цілеспрямованої боротьби зі злочинністю.

Удосконалення боротьби з комп'ютерною злочинністю та іншими правопорушеннями у сфері комп'ютерної інформації має бути направлене на загальну організацію цієї діяльності, у тому числі на розвиток інформаційного законодавства, а також на запобігання комп'ютерної злочинності та активізацію караючої та правовідновної діяльності.

Початковим етапом боротьби з комп'ютерною злочинністю є інформаційно-аналітична робота. Доводиться констатувати, що боротьба з комп'ютерною злочинністю сьогодні ще далека від досконалості. Це пов'язане, у першу чергу, із відсутністю необхідної кримінологічно значимої інформації про її масштаби та поширення, яку отримують у результаті проведення цілеспрямованих і поглиблених досліджень.

Тому на початковому етапі дуже важливо створити дієву та ефективну систему обліку комп'ютерної злочинності, вивчення її «географії» та розробити порядок аналітичної діяльності органів, які здійснюють боротьбу з цими суспільно небезпечними діяннями. Отримані дані в сукупності з іншими відомостями можуть бути покладені в основу більш повного і всебічного аналізу проявів комп'ютерної злочинності, її специфіки та детермінації, а також оцінки попереднього досвіду боротьби з даним явищем. Важливим є прогноз розвитку комп'ютерної злочинності, планування і програмування боротьби з нею, з точним визначенням цілей і завдань цієї діяльності.

Законодавство у сфері комп'ютерної інформації має бути направлене на розвиток міждержавної і внутрішньодержавної законотворчості, що регулює обмін інформацією. Міждержавне інформаційне законодавство включає в себе двосторонні й багатосторонні угоди з державами ближнього і далекого зарубіжжя. Розробка і підписання таких угод забезпечать безпечну інтеграцію України у світовий інформаційний простір.

Велику роль у міжнародному законодавстві щодо захисту від комп'ютерної злочинності відіграла Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. [21], підписана у м. Будапешті, ратифікована Законом України «Про ратифікацію Конвенції про кіберзлочинність» від 07 вересня 2005 р. № 2824-IV (за станом на 14 жов. 2010 р.) [22].

Внутрішньодержавне законодавство полягає у створенні інформаційного законодавства, що відповідатиме всім вимогам сучасності та має бути адаптованим до норм міжнародного права.

Важливу роль у захисті від комп'ютерних злочинів відіграє законодавча робота, спрямована на створення нормативних актів, які регулюють формування, використання і захист інформації конфіденційного характеру. Йдеться про законодавче врегулювання діяльності суб'єктів інформаційного обігу, пов'язаного з персональними даними (відомостями про громадян), комерційною, службовою, банківською, професійною таємницею і т. п. Сьогодні безпека цієї сфери є об'єктом кримінально-правового захисту. Однак визначення понять «охоронювана законом комп'ютерна інформація», «неправомірний доступ до охоронюваної законом комп'ютерної інформації», «шкідлива програма для ЕОМ» та інші законодавчо або не визначені, або носять розмитий, неупереджений характер.

Не зовсім чітко розкрито поняття «сфери комп'ютерної інформації», визначено предмет відносин у даній сфері, суб'єкти цих відносин і їхній соціальний зв'язок. Так, закон може дати такі визначення: охоронювана законом комп'ютерна інформація — це інформація на машинному носії, ЕОМ, системі ЕОМ, мережі ЕОМ, яку ідентифікують ознаками (реквізитами), щодо якої добровільний правовласник інформації встановив відповідний режим захисту та експлуатації. Охоронювана законом інформація ЕОМ — це охоронювана законом комп'ютерна інформація, яка забезпечує функціонування ЕОМ, системи ЕОМ, мережі ЕОМ.

У свою чергу, кримінально караний неправомірний доступ до охоронюваної законом комп'ютерної інформації слід визначити як несанкціоновані або незаконні дії з охороню-

ваною законом комп'ютерною інформацією, які спричинили знищення, блокування, модифікацію, або копіювання інформації, а також порушення роботи ЕОМ, системи ЕОМ або мережі ЕОМ.

Незаконні несанкціоновані дії можуть бути спрямовані на: ознайомлення з охоронюваною законом комп'ютерною інформацією; знищення, блокування, модифікацію, копіювання, адаптацію, декомпілювання охоронюваної законом комп'ютерної інформації.

Слід особливо відзначити важливість координації діяльності суб'єктів боротьби з комп'ютерною злочинністю в її запобіжному, каральному і правовідновному аспектах. Причому взаємодія має ґрунтуватися на чіткому розподілі міжвідомчих і внутрішньовідомчих компетенцій підрозділів, що здійснюють боротьбу з комп'ютерною злочинністю. Наприклад, потрібно чітко визначити поле діяльності в цій сфері підрозділів СБУ та МВС. Так, виключно підрозділи СБУ повинні забезпечувати інформаційну безпеку об'єктів та організовувати контррозвідувальне забезпечення у даній сфері. У свою чергу, до компетенції МВС можуть бути віднесені питання щодо розкрадання шляхом учинення злочинів у сфері комп'ютерної інформації.

Міжвідомча і внутрішньовідомча координація діяльності підрозділів, що здійснюють боротьбу з комп'ютерною злочинністю, та їхня компетенція має бути визначена як на рівні закону, так і відомчими та міжвідомчими нормативними актами.

Важливе значення має посилення співпраці підрозділів, що здійснюють боротьбу з комп'ютерною злочинністю, та суб'єктами інформаційного обігу. Об'єднана протидія комп'ютерним злочинам може здійснюватися тільки на основі ефективної та високопрофесійної роботи підрозділів по боротьбі з комп'ютерними злочинами. Діяльність цих підрозділів необхідно забезпечити відповідною правовою, матеріальною та кадровою підтримкою держави. Ефективна і високопрофесійна діяльність правоохоронних органів повинна поєднуватися з принципами конфіденційності, довірчої взаємодії і гарантіями збереження державної, банкової, комерційної таємниці та інших цінних відомостей.

На стадії запобігання комп'ютерним злочинам важливо, по-перше, змінювати умови зовнішнього середовища таким чином, щоб утруднити чи виключити кримінальне використання комп'ютерної інформації та техніки; по-друге, забезпечувати цілеспрямований позитивний вплив на людей і запобігати тим самим їх кримінальну поведінку в даній сфері.

На державному рівні значима розробка спеціальних систем захисту комп'ютерної інформації загальнодержавного, загальнонаціонального значення, а також створення правової основи їх функціонування. Важливу роль при цьому має відігравати спеціалізоване правове виховання суб'єктів інформаційного обігу, власників і користувачів комп'ютерної інформації та техніки.

Що стосується кримінологічно значущих аспектів правоохоронної діяльності, то необхідно враховувати, що орган дізнання, слідчий, прокурор, суд стикається з підозрюваними і обвинуваченими, які мають спеціальні знання. Тому важливим є підбір фахівців і експертів, технічна та інформаційна підготовка яких сприяла б не тільки вирішенню питань про докази, а й з'ясування причин та умов учинення цих злочинів, вироблення методичних рекомендацій щодо їх запобігання чи усунення.

Список використаних джерел

1. Кримінальний кодекс України: Закон від 5 квіт. 2001 р. (за станом на 12 січ. 2018 р.). *Верховна Рада України.* URL: http://zakon3.rada.gov.ua/laws/show/2341-14.

2. Збірник методичних рекомендацій щодо протидії кіберзлочинам. Ч. 1. Розкриття та розслідування кіберзлочинів / О. Є. Користін, С. А. Лебідь, Ю. Ю. Орлов, А. В. Савченко, В. В. Топчій, Л. Д. Удалова та ін. / за заг. ред. О.М. Джужі. Київ: Нац. акад. внутр. справ, 2010. 219 с.

3. Козак Н. С. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Збірник наукових праць Ірпінської фінансово-юридичної академії (економіка, право)*. 2013. № 2. URL: http://nbuv.gov.ua/UJRN/znpifyua_2013_2_26.

4. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия. М, 1996. С. 16–18.

5. Кримінальний кодекс Української РСР від 28 грудня 1960 року (введений в дію з 1 квіт. 1961 року; втратив чинність з 1 вер. 2001 р.) URL: http://zakon0.rada.gov.ua/laws/show/2001-05.

6. Шахов А. В. Электронные взломщики-преступники под маской романтиков. *Оборудование, системы, технологии*. 1997. Март — апрель. С. 89–93.
7. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: Луган. держ. ун-т внутр. справ, 2012. 327 с.
8. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / Б. В. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов; за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с.
9. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.; за заг. ред. В. В. Коваленка. К.: Видавничий дім «Скіф», 2012. 728 с.
10. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні: монографія / за заг. ред. О. М. Литвинова. Харків, 2016. 212 с.
11. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ, 2007. 304 с.
12. Головкін Б. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинність). *Кримінологія*: підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін.; за ред. В. В. Голіни, Б. М. Головкіна. Харків: Право, 2014. Р. 23. С. 293–303.
13. Бутузов В. М. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Київ, 2007. № 17. С. 316–325.
14. Гавловський В. Д. Деякі сучасні проблеми протидії комп'ютерній злочинності та комп'ютерному тероризму. Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ, 2009. № 19. С. 247–252.
15. Кузьменко Б. В., Заїка Ю. О. Кібертероризм: світові й українські реалії. *Наук. вісн. Нац. акад. внутр. справ*. Київ, 2012. № 2 (81). С. 92–98.
16. Науково-практичний коментар Кримінального кодексу України / Д. С. Азаров, В. К. Грищук, А. В. Савченко та ін.; за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. Київ, 2016. 1064 с.
17. Андрушко П. П. Коментар до розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), системи та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України. *Законодавство України*. 2005. № 3. С. 65–87.
18. Бутузов В. М., Остапець С. Л., Шеломненцев В. П. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: наук.-практ. комент. Київ, 2005. 86 с.
19. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 лип. 1994 р. № 80/94-вр (за станом на 19 квіт. 2014 р.). *Верховна Рада України*. URL: http://zakon0.rada.gov.ua/laws/show/80/94-вр.
20. Кодекс України про адміністративні правопорушення: Закон від 7 груд. 1984 р. № 8073-X (за станом на 07 січ. 2018 р.). *Верховна Рада України*. URL: http://zakon5.rada.gov.ua/laws/show/80731-10.
21. Конвенція Ради Європи про кіберзлочинність від 23 листоп. 2001 р. (м. Будапешт) (ратифікована Законом України від 07 вер. 2005 р. № 2824-IV (за станом на 14 жов. 2010 р.). *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/994_575.
22. Про ратифікацію Конвенції про кіберзлочинність: Законом України від 07 вер. 2005 р. № 2824-IV (за станом на 14 жов. 2010 р.). *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/2824-15.

Топчий Виталий Васильевич,
кандидат юридических наук,
прокурор отдела прокуратуры Киевской области
(Прокуратура Киевской области)

Тычина Дмитрий Михайлович,
кандидат юридических наук,
старший научный сотрудник
(Национальная академия внутренних дел)

ПРЕДОТВРАЩЕНИЕ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

В статье рассмотрены проблемные вопросы компьютерной преступности (киберпреступлений); формирование информационного пространства, основанного на использовании электронно-

вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи; защиты компьютерной информации от несанкционированного (незаконного) вмешательства действующего законодательства в этой сфере; мер по обеспечению защиты информационного пространства в государстве.

***Ключевые слова**: компьютерные преступления; киберпреступления; компьютерная преступность; компьютерная информация; информационное пространство; электронно-вычислительные машины (компьютеры) компьютерные системы и сети; сети электросвязи; меры по обеспечению защиты информационного пространства.*

Topchiy Vitaly Vasilyevich,
Candidate of Law Sciences
Prosecutor of the Prosecutor's Office of the Kyiv region
(Prosecutor's Office of the Kiev region)

Tichina Dmitry Mikhailovich,
Candidate of Law Sciences,
Senior Research Fellow
(National Academy of Internal Affairs)

PREVENTION OF THE USE OF MODERN INFORMATIONTECHNOLOGY FOR CRIMINAL GOALS

Computer crimes are a new type of socially dangerous acts, and their definition must be given in the light of the feature that is the basis of the current classification of crimes. It is the concept of crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks (computer crimes) can be formulated as socially dangerous, unlawful, criminal, guilty acts that cause harm. information relations, a means of ensuring the normal functioning of which are electronic computers, automated systems, computer networks or telecommunication networks. Such crimes should include crimes provided for in Articles 361 — 363-1 of the Criminal Code of Ukraine.

In the opinion of N. S. Kozak, the urgency of the investigation of computer crimes is due to the fact that the peculiarities of the formulation of the norms of the Criminal Code of Ukraine concerning these crimes to some extent complicate, and in some cases, practically make their application impossible, they cause ambiguous understanding by law enforcement and judicial authorities, that leads to errors in the qualification of these crimes [3].

The emergence of the first computer crimes and the further growth of computer crime were due to the transition to automated systems of document circulation.

The processes of automation of banking activities determined a qualitatively new stage in the growth of computer crime.

Favorable conditions for the implementation of computer crimes and the social situation of that period are characterized by active market transformations and the massive impoverishment of a large part of the population of the country, which identified the causes and conditions (determinants) for committing these socially dangerous acts that are embodied in the motivation of criminals.

Most computer crimes were committed to enrich. Of the total number of reported and analyzed crimes, 52 % were associated with theft of funds, 16 % — with destruction and destruction of computer software, 12 % — with deliberate distortion of source data, 10 % — with theft of information and programs, 10 % — with stealing services [6].

The improvement of the fight against computer crime and other violations in the field of computer information should be directed at the overall organization of this activity, including the development of information legislation, as well as the prevention of computer crime and the activation of punitive and legal activities.

The initial stage in the fight against computer crime is information and analytical work.

Therefore, at an early stage, it is very important to create an effective and effective computer crime accounting system, studying its «geography» and develop an analytical framework for the bodies that carry out the fight against these socially dangerous acts.

Legislation in the field of computer information should be directed to the development of interstate and domestic lawmaking, which regulates the exchange of information.

An important role in protecting against computer crime is played by the legislative work aimed at creating normative acts that regulate the formation, use and protection of confidential information. It is about the legislative regulation of the activities of information circulation subjects connected with personal data (information about citizens), commercial, official, banking, professional secrets, etc.

At the stage of prevention of computer crimes, it is important, firstly, to change the conditions of the environment in such a way as to make it difficult or impossible to criminalize the use of computer information and technology; and secondly, to ensure targeted positive impact on people and thereby prevent their criminal behavior in this area.

At the state level, it is important to develop special systems for the protection of computer information of national, national significance, as well as the creation of the legal basis for their functioning. An important

role in this must play a specialized legal education of information circulation subjects, owners and users of computer information and technology.

With regard to the criminologically significant aspects of law enforcement, it must be borne in mind that the inquiry authority, investigator, prosecutor, court faces suspects and defendants who have special knowledge. Therefore, it is important to select experts and experts whose technical and informational training would contribute not only to solving questions of evidence, but also to clarify the causes and conditions for the commission of such crimes, and to develop methodological recommendations for their prevention or elimination.

Key words: *computer crimes; cybercrime computer crime; computer information; information space; electronic computers (computers); computer systems and networks; telecommunication network; precautions to ensure the protection of the information space.*

Надійшла до редколегії 22.03.2018