УДК 343.2
DOI https://doi.org/10.32850/sulj.2019.4.2.18

ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ ВІДНОСИНИ ЯК НОВИЙ КРИМІНАЛІСТИЧНИЙ ОБ'ЄКТ

Стратонов В. М.

У роботі розглядаються криміналістичні, кримінально-правові проблеми, пов'язані з комп'ютерною злочинністю в Україні. Актуалізуються окремі питання захисту інформаційних відносин, застосування комп'ютерних технологій відповідно до законодавства України порівняно із законодавством деяких інших країн. Головною метою роботи є актуалізація питань щодо розслідування злочинів, які вчиняються за допомогою комп'ютерних технологій. Обґрунтовується питання щодо визначення об'єктів злочинних посягань у системі розслідування комп'ютерних злочинів з урахуванням міжнародної практики.

Ключові слова: *захист інформації, об'єкт розслідування, автоматизовані системи, технічний захист, криміналістика.*

В работе рассматриваются криминалистические, уголовно-правовые проблемы, связанные с компьютерными преступлениями в Украине. Актуализируются некоторые вопросы касательно защиты информационных отношений, возникающих в процессе использования компьютерных технологий в соответствии с законодательством Украины. Анализ проводится в сравнении с законодательством некоторых других стран. Основной целью работы является актуализация вопросов расследования преступлений, которые совершаются с помощью компьютерных технологий. Главная цель работы – характеристика объектов уголовных преступлений в системе расследования с учетом международной практики.

Ключевые слова: *защита информации, объект расследования, автоматизированные системы, техническая защита, криминалистика.*

Currently, there are no common concepts of the characteristics of ways of committing computer crimes, their specific names and classification in the domestic and foreign forensic science. This problem is quite new to the science as it is still only in the stage of comprehension and theoretical development.

Unfortunately, together with positive achievements, informatization, like any social phenomenon, has negative manifestations: the ability to use digital technology to commit crimes. Considering this, it is fundamentally important to investigate means of committing crimes in the field of information technology.

Hereby it deals with forensic, criminal and legal issues related to computer crimes in Ukraine. There are some issues related to the protection of information relations using computer technologies are submitted in accordance with the laws of Ukraine compared to the laws of some other countries. The main purpose of the work is to reveal the matters of the investigation of crimes committed with the help of electronic means of data proceedings. There was also justified the problem of determining objects of criminal offenses in the cyber crime investigation system based on international practice.

However, attaching certain rules in our legislation don't solve the problems. Issues emerge in the direct implementation of these norms in everyday life, since investigation authorities do not only apply technical devices and information technologies in their activities, but they also don't possess necessary information. Hence, they is a call to explain more precisely a number of special terms related to information technology, which is important in describing information relations.

We pay attention on the meaning of "information" as a new forensic object and a specific object of legal regulation and the concepts associated with that; then considering the set of detailed legislation with regard to information relations in Ukraine and determining the state of legal support in the matter herewith. We characterize the most important definitions related to a special tool for information processing – the computer. This sequence will allow to use the new special terminology in compiling the forensic characteristics of crimes in the field of computer information and identifying the objects of crime more freely.

Key words: *information security, object of investigation, automated systems, technical protection, forensic science.*

Постановка проблеми та її актуальність. Рубіж XX і XXI ст. знаменується переходом високорозвинених у технічному відношенні країн до нової постіндустріальної фази свого розвитку – інформаційного суспільства, у якому у діяльності людей, як продукт праці, домінують автоматизовані електронно-обчислювальні системи (далі – ЕОС). Впровадження і використання сучасних комп'ютерних технологій, розвиток глобальної комп'ютерної мережі Internet, безумовно, сприяє розв'язанню політичних і соціальних проблем нашої держави. Водночас це зумовило виникнення нових злочинів, пов'язаних із порушенням роботи автоматизованих ЕОС, викраденням, привласненням, вимаганням або шахрайським заволодінням інформацією (далі – злочинів у сфері використання комп'ютерних технологій).

Виходячи зі стратегічного курсу України на інтеграцію у світовий інформаційний простір, виникає потреба з'ясування й усвідомлення всіх позитивних і негативних явищ інформаційної цивілізації: впровадження інформаційних технологій на основі комп'ютерної техніки у всі сфери суспільного життя.

Метою роботи є актуалізація питань щодо розслідування злочинів, зокрема нового об'єкта у кримінальному праві, а саме інформації та інформаційних процесів.

Виклад основного матеріалу. Поряд із позитивними здобутками інформатизація, як і будь-яке соціальне явище, має і негативні прояви: можливість використання комп'ютерних технологій для вчинення правопорушень, зокрема злочинів, у т. ч. організованими злочинними формуваннями. Тобто інформатизація має двоякий суспільний ефект:

1. Лібералізація суспільних і міждержавних відносин породила зростання загроз для суспільних відносин в інформаційній сфері з боку транснаціональних злочинців.

2. Кризовий стан економіки в нашій країні змусив звернути увагу суспільства до застосування новітніх технічних засобів обробки інформації – комп'ютерних систем і засобів зв'язку, переважно іноземного виробництва. Це викликано поширенням можливостей несанкціонованого доступу до інформації в таких інформаційних системах [1, с. 4], що, у свою чергу, визначило необхідність протидії протиправним, у т. ч. злочинним, посяганням на інформаційні та інші відносини, які охороняються державою: захисту інформації в автоматизованих (комп'ютерних) системах – глобальних, континентальних, регіональних, локальних, у рамках окремих держав, установ, організацій тощо.

Як свідчать дослідження, злочинні (в т. ч. організовані) формування не стоять осторонь досягнень науково-технічного прогресу. Вони, маючи значні фінансові ресурси, здобуті незаконним шляхом, активно використовують новітні інформаційні технології для реалізації своїх протиправних посягань. Загалом кримінальне використання сучасних інформаційних технологій робить «комп'ютерну злочинність» не тільки дуже прибутковою, але і небезпечною справою. І не даремно Підкомітет ООН із питань злочинності ставить цю проблему в один ряд із тероризмом і наркотичним бізнесом.

Необхідно зауважити, що сьогодні ця проблема зрозуміла насамперед володільцям, користувачам комп'ютерної техніки та їх систем і, звичайно, працівникам правоохоронних органів, державним органам. Тому проведений всебічний аналіз вітчизняного законодавства, яке регулює суспільні інформаційні відносини в Україні, дозволяє стверджувати, що наша держава, поряд із заходами стимулювання розвитку інфраструктури на основі комп'ютерних технологій, вживає заходи превентивного характеру щодо їх використання у злочинних цілях. Свідченням цього є окрема глава у кримінальному кодексі України, присвячена злочинам із використанням ЕОМ, систем і комп'ютерних мереж і електрозв'язку [2, с. 359–360].

Закріплення в законодавстві певних норм не вирішує проблем. Проблеми виникають у безпосередній реалізації цих норм у повсякденному житті, а саме:

1. Нагальною потребою є напрацювання методів, методик виявлення і розкриття традиційних правопорушень, що вчинюються за допомогою комп'ютерних технологій, а також злочинів, передбачених ст. 361–3631 Кримінального кодексу України.

2. Особливо актуальною є проблема оволодіння практичними працівниками правоохоронних органів новими знаннями щодо кваліфікації злочинів, що вчинюються з використанням комп'ютерних технологій.

3. Несвоєчасне повідомлення про інформаційні злочини. Мабуть, ніхто у світі не має сьогодні повної картини інформаційної злочинності. Зрозуміло, що державні і комерційні структури, які піддалися нападам, не дуже схильні афішувати наслідки, заподіяні нападами, й «ефективність» своїх систем захисту. Тому випадки злочинів стають надбанням гласності далеко не завжди. Але і ті факти, що відомі, справляють сильне враження [3, с. 2–4].

Так, в Італії у 1983 р. за допомогою комп'ютерів було викрадено з банків більш 20 млрд лір. У Франції втрати досягають 1 млрд франків на рік, і кількість подібних злочинів збільшується на 30–40% щорічно. У Німеччині комп'ютерна мафія викрадає за рік до 4 млрд євро. За даними Американського національного центру інформації з комп'ютерної злочинності, за 1988 р. комп'ютерна злочинність нанесла американським фірмам збитки в розмірі 500 млн доларів.

А всього (за поверхневими підрахунками) щорічні втрати від «комп'ютерної злочинності» у Європі й Америці складають кілька десятків мільярдів доларів. У 90% випадків детективам навіть не вдається вийти на слід злочинця. І це в Америці, де перше подібне правопорушення було зафіксовано ще в 1966 р., і поліція вже накопичила деякий досвід у цьому напрямі.

У 1991 р. відбулося викрадення 125,5 тис. американських доларів у Зовнішекономбанку. Злочинці з числа співробітників обчислювального центру Банку відкрили декілька особистих рахунків за підробленими паспортами і почали переведення зазначених коштів на них, але були затримані [4, с. 157–160].

Влітку 1992 р. представник одного закордонного алмазного концерну скопіював на свої дискети інформацію з комп'ютерної мережі алмазодобувного об'єднання Росії, оцінену як службова таємниця [5, с. 34].

У вересні 1993 р. була здійснена спроба «електронного шахрайства» на суму більш 68 млрд рублів. У тому ж місяці в одному з комерційних банків відбулося розкрадання програмного забезпечення системи електронних платежів, що припускала застосування кредитних карток.

Навесні 1996 р. злочинці намагалися впровадити в банківську комп'ютерну систему Москви підроблені векселі з реквізитами Московського ощадного банку, аби викрасти 375 млрд рублів і 80 млн доларів США [6, с. 3–6].

«Комп'ютерна злочинність» – це не лише розкрадання грошей. Це і «витівки» з електронними вірусами. Значні і ніким не зумовлені точно, втрати виникають внаслідок поширення шкідливих програм.

На ринку програмного забезпечення в Україні щомісяця фіксується поява від 2 до 10 нових вірусів. Аналогічні проблеми виникають і в країнах Європи. Програмісти повідомили, що сьогодні по комп'ютерах кочує близько 5 тис. різновидів вірусів, щотижня з'являється близько 5 нових їхніх різновидів, і велика частина цієї «інфекції» створюється в межах України та держав пострадянського простору [7, с. 51–73]. Ступінь небезпеки можна проілюструвати кримінальною справою, порушеною прокуратурою Литви в 1992 р. Тоді «електронна зараза» потрапила до комп'ютера Ігналінської атомної електростанції, що привело до виводу з ладу захисної системи. Такі дії могли спровокувати аварію, і міг би бути другий Чорнобиль.

Програміст однієї з фірм, яка спеціалізується на розробці програмного забезпечення для ЕОМ, прокоментував ситуацію так: «Упевнений, що при тотальній криміналізації нашого суспільства «комп'ютерна злочинність» не стала ще в Україні національним нещастям лише через не менш тотальну технічну відсталість». Доволі слушна думка.

Водночас у США в 1996 р. Інститутом захисту комп'ютерів разом із ФБР було проведене дослідження, спрямоване на визначення поширеності комп'ютерних злочинів і заходів, прийнятих для їхнього запобігання. Відповіді були отримані із 428 організацій. Опитування показало таке: понад 50% опитаних відповіли, що не мають плану дій на випадок мережного вторгнення. Понад 60% не мають стратегії збереження доказів для подальшого судового розгляду криміналь-

них чи цивільних справ. Понад 70% респондентів не мають пристроїв, які попереджають про вторгнення в їхню комунікаційну й інформаційну системи. Менш 17% зазначили, що вони повідомлять правоохоронні органи у випадках нападу на інформаційні системи (ІС). Наведені дані наочно характеризують тенденції росту комп'ютерної злочинності та своєчасність реакції вітчизняного законодавця на зростання суспільної небезпеки цього виду правопорушень [8, с. 234].

Основна проблема сучасного етапу, імовірно, полягає в рівні спеціальної підготовки посадових осіб правоохоронних органів, котрі мають втілювати в життя вимоги нових законів.

Надаючи криміналістичні рекомендації у сфері інформаційних правовідносин, варто враховувати різнорідність складу й освітній рівень нашого слідчо-судового апарату. Ясно, що є вже і добре підготовлені фахівці. Але багато співробітників органів слідства і дотепер не тільки не використовують технічні засоби й інформаційні технології у своїй діяльності, але і недостатньо інформовані про них.

Ці розуміння змушують трохи більш детальніше дати пояснення цілому ряду спеціальних термінів, які належать до сфери інформаційних технологій і є важливими в описі інформаційних відносин. Також варто дати криміналістичну характеристику злочинам цього виду.

Для цього необхідно насамперед усвідомити зміст поняття «інформації» як нового криміналістичного об'єкта й особливого об'єкта правового регулювання і понять, із ним пов'язаних, розглянути сукупність нормативного регулювання в Україні інформаційних відносин і визначити стан правового забезпечення ситуації, що складається у цій сфері. Потім необхідно розглянути найбільш важливі терміни, що стосуються спеціального інструмента обробки інформації – комп'ютера. Така послідовність дозволить надалі більш вільно користатися новою спеціальною термінологією при складанні криміналістичної характеристики злочинів у сфері комп'ютерної інформації.

Вітчизняні та закордонні видання і засоби масової інформації останніх років заповнені різними поняттями, що позначають ті чи інші нові прояви кримінального характеру в інформаційній сфері. Зустрічаються найменування і «комп'ютерні злочини», і «комунікаційні злочини», і «кібербандитизм». Злочинців іменують «хакери», «кракери», «кіберпанки», «бандити на інформаційних супермагістралях». Розходження в термінології вказує не лише на стурбованість суспільства новою погрозою, але і на відсутність повного розуміння суті цієї погрози. Поступово на наших очах виникла інформаційна індустрія, чия самостійність і перспектива розвитку цілком залежали від точного регулювання правовідносин, що виникають при формуванні та використанні інформаційних ресурсів. «Інформаційна революція» розпочалася для України у складний економічний і політичний період і вимагала термінового регулювання виникаючих на її шляху проблем.

Тим часом, як відомо, правові механізми можуть бути включені та стають ефективними лише тоді, коли суспільні відносини, що підлягають регулюванню, достатньою мірою стабілізувалися.

Сьогодні, коли створений і прийнятий ряд базових нормативних актів у сфері інформаційних відносин, настав час для їхнього застосування на практиці, однак на цьому шляху неминучі проби і помилки. І якщо такі помилки, допущені, наприклад, у сфері господарських відносин, можуть бути тим чи іншим способом ефективно виправлені, то помилки у кримінально-репресивній сфері відображаються на конституційних правах і свободах конкретних громадян і мають незворотний характер.

Інформаційні правовідносини – це відносини, що виникають при: формуванні та використанні інформаційних ресурсів на основі створення, збору, обробки, накопичення, збереження, пошуку, поширення і представлення споживачу документованої інформації; створення і використання інформаційних технологій і засобів їхнього забезпечення; захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації.

Аналіз чинного законодавства показує, що: інформацією є сукупність призначених для передачі формалізованих знань про осіб, предмети, факти, події, явища і процеси, незалежно від форми їхнього представлення (Закон України «Про інформацію»).

Правовому захисту підлягає тільки документована інформація, тобто інформація, убрана у форму, яка дозволяє її ідентифікувати (Закон України «Про інформацію»). Документована інформація є об'єктом цивільних прав і має власника. Інформація, ознайомлення з якою обмежується її власником чи відповідно до законодавства, може бути конфіденційною, а призначена для необмеженого кола осіб – масовою. Обмеження (установлення режиму) використання інформації визначаються законом чи власником інформації, що повідомляють про ступінь (рівень) її конфіденційності.

Конфіденційними відповідно до закону є, зокрема, такі види інформації, як державна таємниця [9], таємниця листування, телефонних переговорів, поштових, телеграфних чи інших повідомлень [10], таємниця усиновлення, службова таємниця, комерційна таємниця, банківська таємниця, особиста таємниця, сімейна таємниця, інформація, що є об'єктом авторських і суміжних прав, інформація, що безпосередньо торкається прав і свобод громадянина, чи персональні дані тощо [11].

Будь-яка форма заволодіння і користування конфіденційною документованою інформацією без прямо вираженої згоди її власника (за винятком випадків, прямо зазначених у законі) є порушенням його прав, тобто неправомірним. Неправомірне використання документованої інформації підлягає покаранню.

Також ми бачимо, що інформаційні відносини одержали і кримінально-правовий захист, інформація й інформаційні відносини стали новим об'єктом злочину.

Тим часом у вітчизняній криміналістичній науці усе ще не існує чіткого визначення поняття комп'ютерного злочину. Складність у формулюванні цих понять існує, очевидно, як через неможливість виділення єдиного об'єкта злочинного зазіхання, так і через множинність предметів злочинних посягань із погляду їхньої кримінально-правової охорони.

Одна частина дослідників відносить до комп'ютерних злочинів дії, у яких комп'ютер є або об'єктом, або знаряддям зазіхань.

Дослідники ж другої групи відносять до комп'ютерних злочинів лише протизаконні дії у сфері автоматизованої обробки інформації. Як головна ознака, що дозволяє віднести ці злочини у відособлену групу, виділяється спільність способів, знарядь, об'єктів зазіхань.

Іншими словами, об'єктом посягання є інформація, оброблювана в комп'ютерній системі, а комп'ютер є знаряддям посягання. Необхідно відзначити, що законодавство багатьох країн, у т. ч. й в Україні, стало розвиватися саме цим шляхом.

Щодо об'єкта злочинного зазіхання двох думок бути не може – ним, природно, є інформація, а дії злочинця варто розглядати як замах на інформаційні відносини суспільства.

Але далі необхідно врахувати, що, якщо інформація є не об'єктом, а засобом замаху на інший об'єкт кримінально-правової охорони, то тут необхідно робити розходження в тім, чи була це машинна інформація, тобто інформація, яка є продуктом, виготовленим за допомогою чи для комп'ютерної техніки, або вона мала інший, «некомп'ютерний» характер.

Тому необхідно відразу усвідомити, що під машинною інформацією розуміється інформація, яка циркулює в обчислювальному середовищі, зафіксована на фізичному носії у формі, доступній сприйняттю ЕОМ, чи передається по телекомунікаційних каналах: сформована в обчислювальному середовищі та переправлена за допомогою електромагнітних сигналів з однієї ЕОМ в іншу, з ЕОМ на периферійний пристрій або на керуючий датчик устаткування [12, с. 3–10].

Засоби комп'ютерної техніки за своїм функціональним призначенням можна підрозділити на дві основні групи:

1) апаратні засоби (Hard Ware);

2) програмні засоби (Soft Ware).

Під апаратними засобами комп'ютерної техніки розуміються технічні засоби, які використовуються для обробки даних: механічне, електричне й електронне устаткування для обробки інформації. До них належать:

1) Персональний комп'ютер (ПЕОМ чи ПК) – комплекс технічних засобів, призначених для автоматичної обробки інформації у процесі рішення обчислювальних та інформаційних задач.

2) Периферійне устаткування – устаткування, яке має підлеглий кібернетичний статус в інформаційній системі: будь-який пристрій, що забезпечує передачу даних і команд між процесором і користувачем щодо визначеного центрального процесора, комплекс зовнішніх пристроїв ЕОМ, які не перебувають під безпосереднім керуванням центрального процесора.

3) Фізичні носії магнітної інформації [13, с. 377].

Висновки. Проблема розгляду інформації та інформаційних правовідносин як нового криміналістичного об'єкта полягає, передусім, у тому, що досі чітко не наведено визначення поняття «криміналістичний об'єкт». Зазвичай криміналістична наука, не виробивши до кінця визначення об'єктів, які мають криміналістичне значення, користується переважно кримінальною процесуальною термінологією: доказ, джерело доказів або об'єкти – носії доказової інформації. Криміналістика має справу тільки з реальними фактами, котрі можна виявити за допомогою спеціальних засобів, прийомів і методів, відповідним чином їх зафіксувати та досліджувати. Але інформація, що не є матеріальним об'єктом, цілком відповідає цим вимогам, отже, може бути криміналістичним об'єктом.

Розслідування комп'ютерних злочинів істотно відрізняється від розслідувань інших «традиційних» злочинів. Вивчення кримінальних справ цієї категорії дає підставу думати, що однією з істотних причин низької якості слідства є відсутність систематизованих і відпрацьованих методів розслідування комп'ютерних злочинів, а також помилки при проведенні слідчих дій щодо комп'ютерної інформації або самих комп'ютерів.

Необхідно ввести змішану класифікацію інформаційних злочинів, яка б враховувала й особливості злочинів скоєних за допомогою засобів ЕОТ і цифрового зв'язку, й особливості родових об'єктів інформаційних злочинів:

а) інформаційні злочини, вчинені за допомогою електронно-технологічних засобів:

1) комп'ютерні злочини – злочини передбачені ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України, а також інформаційні злочини, передбачені іншими статтями КК України, які скоєні за допомогою ЕОМ;

2) телекомунікаційні злочини – інформаційні злочини, визначені статтями КК України, скоєні за допомогою інших електронно-технологічних засобів (наприклад, мобільних телефонів чи систем супутникового зв'язку; до таких злочинів можуть належати роумерське шахрайство, розкрадання трафіка телефонних з'єднань, незаконне надання послуг електрозв'язку тощо);

б) інформаційні злочини, скоєні без допомоги електронно-технологічних засобів:

1) інформаційні злочини проти особистості – злочини, визначені ст. 132, 145, 159, 163, 168, 171, 176, 177 КК України;

2) економічні інформаційні злочини – злочини, передбачені ст. 231, 232, 232-1, 232-2 КК України;

3) інформаційні злочини проти громадської безпеки – злочини, передбачені ст. 238, 259 КК України;

4) інформаційні злочини проти національної безпеки та держаних інтересів – злочини, зафіксовані ст. 111, 114, 238, 330, 422 КК України;

5) інформаційні злочини проти органів державної влади, місцевого самоврядування та правосуддя – злочини, передбачені ст. 359, 381, 383, 387 КК України.

Подібна класифікація дозволить поглянути на інформаційні злочини як на цілісну взаємопов'язану систему, а не набір окремих злочинів, пов'язаних із явищем інформації.

З огляду на специфіку, зумовлену особливостями пошуку, збирання та дослідження доказів певного типу, для вирішення криміналістичних завдань, оскільки інформація та інформаційні правовідносини є новим криміналістичним об'єктом, криміналістична характеристика інформаційних злочинів виглядає таким чином:

а) відомості про предмет злочинного посягання: вид і цільове призначення інформації, проти якої спрямований злочин, використовувані матеріальні носії для зберігання й обробки цієї інформації;

б) відомості про середовище вчинення злочину: вид і особливості апаратного, програмного й інформаційного забезпечення автоматизованої інформаційної системи, у якій вчинено злочин, встановлений порядок його функціонування і технологічна схема обробки та захисту інформації відповідно до цільового призначення автоматизованої інформаційної системи;

в) відомості про особистість злочинця: стать, вік, освіту, типовий склад і схему взаємозв'язків у злочинній групі;

г) типову мотивацію і цілеспрямованість злочинного поводження при вчинені злочинів у сфері інформації;

д) типові способи підготовки та вчинення злочину, способи його приховання, у т. ч. типові знаряддя (засоби);

е) відомості про типові обставини вчинення злочину: обстановку, час, місце, виконувану технологічну операцію при обробці інформації;

ж) відомості про сліди вчиненого злочину і типові наслідки злочинів;

з) сукупність (характеристику) вихідної інформації на початку розслідування злочину.

Література

1. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Запоріжжя : Просвіта, 2001. 252 с.

2. Кримінальне право України. Загальна та особлива частина : навчальний посібник / за заг. ред. В.М.Стратонова. Київ: Істина, 2007. 400 с.

3. Аналітичний огляд НЦБ Інтерполу в Україні «Про досвід правоохоронних органів США по боротьбі з комп'ютерною злочинністю». Інформаційний лист МВС від 4 квітня 1997 р. 24 с.

4. Голубєв В.О. Проблеми попередження та розкриття комп'ютерної злочинності у сфері банківської діяльності. *Матеріали 2-ї Міжрегіональної науково-практичної конференції «Концепція формування законодавства України»*. Запоріжжя, 1997. С. 157–160.

5. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. Москва : *Право и Закон*, 1996. 201 с.

6. Компьютерные преступления и обеспечение безопасности ЭВМ. *Проблемы преступности в капиталистических странах*. 1983. № 6. С. 3–6.

7. Кащеев В.И. Специальная техника контроля и защиты информации. *Системы безопасности*. 1995. № 1. С. 51–73.

8. Computer Crim: A Crime fighter's Handbook. D. Icove, K. Seger, W. Von Sorsh. O'Reylli &Associates, Ins., 1995. 437 p.

9. Закон України «Про захист інформації в автоматизованих системах». *Відомості Верховної Ради України*. № 31. 1994. 286 с.

10. Конституція України від 28 червня 1996 р. Київ : ЮРІНКОМ. 1996.

11. Закон України «Про інформацію». *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

12. Проблемы борьбы с компьютерной преступностью. *Борьба с преступностью за рубежом*. 1992. № 4. С. 3–10.

13. Фигурнов В.Э. IBM PC для пользователя. Москва: ИНФРА, 1997. 479 с.

Стратонов В. М.,
доктор юридичних наук, професор,
професор кафедри галузевого права
Херсонського державного університету