

## Особливості порушення кримінальних справ про комп'ютерні злочини



**І. В. Європіна,**  
здобувач Академії адвокатури  
України

Успішне розкриття і розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж, а так само й викриття осіб, винних у вчиненні таких злочинів, значною мірою забезпечується обґрунтованим, своєчасним порушенням кримінальної справи і встановленням обставин, що підлягають доказуванню.

Приводами до порушення кримінальної справи у цій сфері, на нашу думку, можуть бути: повідомлення посадових осіб організацій, їх об'єднань; заяви громадян-користувачів; матеріали органів дізнання МВС і СБУ, де є спеціалізовані підрозділи боротьби з організованою злочинністю, зокрема економічною і комп'ютерною; повідомлення в засобах масової інформації тощо. Водночас слід зважити, що в ч. 1 ст. 94 КПК України наводиться вичерпний перелік приводів до порушення кримінальної справи для всіх видів злочинів, у тому числі і «комп'ютерних»:

- 1) заяви або повідомлення підприємств, установ, організацій, посадових осіб, представників влади, громадськості або окремих громадян;
- 2) повідомлення представників влади, громадськості або окремих громадян, які затримали підозрювану особу на місці вчинення злочину або з поличним;
- 3) явка з повинною;
- 4) повідомлення, опубліковані в пресі;
- 5) безпосереднє виявлення органом дізнання, слідчим, прокурором або судом ознак злочину.

Слідча практика засвідчує, що повідомлення про вчинені злочини у сфері комп'ютерних технологій розподіляються у такій пропорції [1, 37]:

- повідомлення посадових осіб підприємств, установ, організацій (близько 40 %);
- заяви громадян (понад 35 %);
- безпосереднє виявлення органами дізнання, слідчими або прокурором даних, які вказують на ознаки злочину (близько 5 %).

Частина 2 ст. 94 КПК України визначає підстави, що є обов'язковими при порушенні кримінальної справи. Справа може бути порушена лише в тих випадках, коли є достатні дані, які вказують на наявність ознак злочину [2, 189–191; 3].

Проте навіть і за таких умов вирішення питання про порушення кримінальної справи вимагає, як правило, ретельної перевірки та оцінки наявних даних. А тому слідчий чи інша уповноважена особа, отримавши повідомлення про вчинений злочин, зобов'язані призначити дослідчу перевірку, порядок і терміни проведення якої передбачені ст. 97 КПК України. Виняток становлять рідкісні епізоди затримання комп'ютерних злочинців із поличним, наприклад, в момент несанкціонованого копіювання конфіденційної інформації або при викраденні

У статті висвітлюється порядок, приводи і підстави порушення кримінальних справ про злочини у сфері використання комп'ютерів, указуються та досліджуються наявні особливості, аналізуються проблеми.

**Ключові слова:** розслідування злочинів, дослідча перевірка, порушення справи, сліди злочину, оперативно-розшукова діяльність, матеріали спеціальних досліджень.

машинних носіїв з такою інформацією, передачі їх третім особам тощо. У цих випадках для невідкладних слідчих дій (особистого обшуку затриманого, обшуку за місцем його роботи та проживання, де знаходиться персональний комп'ютер, тощо), а також для проведення оперативно-розшукових заходів по «гарячих слідах» (в інтересах попередження втрати чи знищення доказів злочину) кримінальна справа порушується невідкладно.

У разі проведення дослідчої перевірки вживаються заходи до встановлення таких необхідних для порушення кримінальної справи даних, як:

- сліди злочину;
- місце неправомірного проникнення в комп'ютерну мережу (зсередини потерпілої організації чи ззовні);
- способи здійснення неправомірного доступу (подолання програмних засобів захисту, вилучення засобів комп'ютерної техніки, маніпуляції з даними, керуючими командами та інформацією, використання шкідливих програмних чи технічних засобів);
- засоби, що використовувались при вчиненні злочину (технічні, програмні, інші);
- способи подолання інформаційного захисту (підбір ключів і паролів, крадіжка паролів, відключення засобів доступу тощо).

Слід відмітити, що копіювання, зміна, модифікація, виток, знищення інформації можуть бути викликані не тільки умисними неправомірними діями, але й помилками, неумисною неправильною поведінкою персоналу організації-жертви, і ці особливості мають бути враховані при вирішенні питання про порушення кримінальної справи та визначенні її кваліфікації за КК України.

Під час дослідчої перевірки проводяться опитування персоналу потерпілої організації (показання цих осіб в подальшому складуть базу свідчень у кримінальній справі) та огляд місця події.

Огляд проводиться в порядку ст. 190 КПК та має своєю метою за допомогою спеціалістів установити, зафіксувати та видалити сліди вчиненого злочину (в подальшому вони можуть бути визнані як речові чи інші докази), а також отримати іншу інформацію, необхідну для порушення кримінальної справи.

**Слідами злочинів** можуть бути:

- при неправомірному доступі до комп'ютерної інформації, системи, мережі або порушення правил її експлуатації;
- сліди, що вказують на зміни в заданій файлової структурі (перейменування каталогів і

файлів, зміна розмірів і змісту файлів, зміна стандартних реквізитів файлів, поява нових каталогів і файлів, видалення з каталогів імен файлів, стирання або додавання окремих записів, фізичне знищення або розмагнічування носіїв інформації, поява нових реєстраційних даних, які комп'ютер робить автоматично тощо);

- сліди, що є результатом роботи антивірусних і тестових програм (наприклад результати роботи програми DrWeb відбиваються у файлі report.web, зміст якого можна легко переглянути);
- сліди, що відбивають зміни в заданій конфігурації комп'ютера (зміна кольору і файлів, поява нових і видалення старих мережних пристроїв, зміна порядку взаємодії з периферійними пристроями (принтером, модемом тощо);
- сліди, що характеризують незвичні прояви в роботі ЕОМ (уповільнене або некоректне завантаження операційної системи, уповільнена реакція машини на введення з клавіатури, уповільнена робота машини з накопичувачами при записі і зчитуванні інформації, неадекватні реакції ЕОМ на команди користувача, поява на екрані нестандартних символів, знаків тощо);
- сліди руху пакетів інформації в мережі Інтернет, де кожний забезпечується адресою комп'ютера-одержувача і шляхом передачі проходить декілька вузлових комп'ютерів (серверів), на яких залишаються сліди реєстрації проходження пакетів і сліди, залишені в результаті неправомірних дій злочинця. Крім того, при відвідуванні Web-вузла браузер (програма) пише електронну адресу цієї сторінки в безліч файлів, що знаходяться на жорсткому диску. Це кеш-файли, файли-сценарії, файли-історії та файли Windows Registry (наприклад, файли-сценарії при перегляді Web-вузла реєструють кожний натиск на мишу і файл, що був використаний як буфер адреси вузлів, які висилали код і зберігають інформацію про це в папці Windows/Cookies; при роботі з Internet Explorer URL файли-історії зберігають послідовність дій оператора в папці Windows/History);
- сліди, що залишаються на «робочому місці» злочинця, так звані сліди засобів для налагодження програм проникнення (наприклад якінебудь рукописні записи – списки паролів, коди, таблиці шифрування, чернетки, роздруквітки тощо);

- сліди, що залишаються на засобах захисту інформації (спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера, пристроях ідентифікації користувача за геометричними ознаками руки, почерку, голосу).
- *при проникненні сторонніх осіб у приміщення, за місцем розміщення комп'ютерного (мережного) устаткування, носіїв інформації та засобів доступу до віддалених мереж (модемів, засобів телефонного і супутникового зв'язку):*
- сліди знарядь зламу, пальців рук, мікрочасток, паперові носії: роздруківки на принтері, записи кодів, паролів тощо.

На описані сліди слід звернути особливу увагу при огляді комп'ютерного (мережного) обладнання та місця події.

**Знаряддями вчинення злочинів** у сфері комп'ютерної інформації виступають засоби комп'ютерної техніки, у тому числі спеціальне програмне забезпечення, за допомогою яких здійснюється безпосередній або опосередкований (віддалений) доступ. До *знарядь безпосереднього доступу* можна віднести носії комп'ютерної інформації (USB Flash накопичувачі, лазерні диски, дискети, касети з магнітною стрічкою для стримера), різноманітне периферійне устаткування (друкуючий пристрій, CD-ROM – накопичувач, стример, дисководи), а також електронні ключі, особисті ідентифікаційні коди тощо.

До *знарядь опосередкованого (віддаленого) доступу* належать, насамперед, мережне устаткування, а також засоби доступу до віддалених мереж (модеми, засоби телефонного і супутникового зв'язку).

Подібно до знарядь можна класифікувати і **способи доступу** до комп'ютерної інформації.

При реалізації *способів безпосереднього доступу* інформація знищується, блокується, модифікується, копіюється, а також може порушуватися робота ЕОМ, системи ЕОМ або їхньої мережі шляхом видання відповідних команд з комп'ютера, на якому інформація знаходиться. Безпосередній доступ може здійснюватися як особами, які працюють з інформацією, так і особами, котрі спеціально проникають у закриті зони та приміщення, де провадиться обробка інформації. Іноді злочинець з метою вилучення інформації, залишеної користувачами після роботи ЕОМ, обстежує робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування (так зване «прибирання сміття») або здійснює перегляд і відновлення стертих програм. Але слід наголосити, що такий спосіб у даний час

менш поширений у зв'язку з тим, що комп'ютерну інформацію легше перехопити при її передаванні телекомунікаційними каналами і комп'ютерними мережами, ніж при безпосередньому проникненні в приміщення.

При реалізації *способів опосередкованого (віддаленого) доступу* до комп'ютерної інформації відбувається підключення до лінії зв'язку законного користувача (наприклад, до телефонної лінії) і одержання тим самим доступу до його системи; проникнення в чужі інформаційні мережі шляхом автоматичного перебору абонентських номерів із наступним з'єднанням із тим або іншим комп'ютером. Перебір здійснюється доти, аж поки на іншому кінці лінії не «озветься» чужий комп'ютер.

Вельми важливими при вирішенні питання про порушення кримінальної справи є **пояснення співробітників (персоналу) організації-жертви**: адміністраторів мережі, інженерів-програмістів, розробників програмного забезпечення та обслуговуючих його осіб, операторів, спеціалістів, що займаються експлуатацією та ремонтом комп'ютерного обладнання, системних програмістів, інженерів засобів зв'язку та телекомунікаційного обладнання, спеціалістів з інформаційної безпеки та ін.

У процесі отримання пояснень з'ясовуються обставини, що передували вчиненню злочину (з метою встановлення кола підозрюваних), обставини виявлення факту злочину (його ознак, способів і засобів, негативних наслідків), наявність та стан функціонування системи інформаційного захисту, її недоліки, інші причини і умови, які могли бути задіяні для вчинення протиправних дій.

*Типовий набір запитань, що потребує пояснень персоналу*, виглядає так:

- чи не було розкрадань носіїв інформації?
- чи не чинив будь-хто із числа працюючих необґрунтованих маніпуляцій з інформацією?
- чи не було порушень заданого режиму функціонування комп'ютерних систем, мереж, комп'ютерів або іншого обладнання?
- чи не було випадків спрацьовування засобів захисту комп'ютерних систем, мереж, обладнання та інформації, котра в них оброблюється?
- чи не з'явилися в приміщенні, де розташовані технічне устаткування, ЕОМ, інші засоби комп'ютерної техніки та носії інформації, сторонні особи (радіотелемеханік, зв'язківець, працівники позавідомчої охорони, санепідемстанції, енергонагляду тощо)?

- чи не було порушень правил ведення журналів обліку часу роботи комп'ютерних систем, мереж, обладнання?
- чи не виявлялось будь-ким інтересу до інформації, яка не належить до їхньої безпосередньої діяльності?
- що відомо про вчинений злочин, підозрюваних осіб, підготування злочину, з яких джерел виходить ця поінформованість?
- яка інформація зазнала впливу, її призначення та зміст?
- які розміри збитку від впливу на інформацію і наслідки, які можуть спричинити шкідливі для ЕОМ, системи ЕОМ та їх мережі програми та технічні засоби?

У випадках, коли персоналом організації-жертви (як правило, співробітниками служби безпеки) самостійно проведена перевірка зі встановлення осіб, причетних до злочину, та окреслено коло підозрюваних осіб, у ході дослідчої перевірки проводиться комплекс оперативно-розшукових та інших заходів щодо підозрюваної особи (групи осіб) і, по можливості, затримання її з поличним (наприклад, у момент отримання в установі банку чи банкоматі викрадених грошових сум; або замовлених через Інтернет речей, придбаних на викрадені «електронні гроші», тощо). Інколи при затриманні вилучаються комп'ютерне обладнання, носії інформації, на яких містяться сліди вчиненого злочину, при цьому спеціалістами проводиться лабораторне дослідження вмісту вилученого.

Результатом проведення дослідчої перевірки, за наявності приводів і підстав, зазначених у ст. 94 КПК України, має стати порушення кримінальної справи за відповідною статтею КК України та подальше розслідування у ній.

Якщо на момент порушення кримінальної справи буде встановлено особу, котра вчинила злочин, кримінальна справа повинна бути порушена щодо цієї особи.

Після порушення справи:

- 1) прокурор направляє справу для проведення досудового слідства за підслідністю, яка визначається в порядку ст. 112 КПК України;
- 2) слідчий приступає до провадження досудового слідства.

У разі, коли кримінальну справу порушено щодо певної особи, слідчий (прокурор, суддя) вправі прийняти рішення про заборону такій особі виїжджати за межі України до закінчення досудового розслідування чи судового розгляду, про що виноситься мотивована постанова (ст. 98-1 КПК України).

Після порушення кримінальної справи прокурор або слідчий зобов'язані вручити копію постанови особі, щодо якої порушено справу, та потерпілому негайно. За неможливості негайного вручення копія постанови вручається не пізніше трьох діб з моменту її винесення.

Якщо неможливо вручити зазначеним особам копію постанови про порушення кримінальної справи протягом строків, визначених ч. 1 ст. 98-2 КПК України, через їх хворобу, неможливість встановлення місця перебування чи з інших поважних причин, копія постанови вручається протягом трьох діб з моменту явки, приводу чи встановлення місця перебування цих осіб. Якщо особа відмовляється одержати копію постанови про порушення кримінальної справи, прокурор або слідчий, складають відповідний протокол.

Представнику потерпілого, захиснику або законному представнику підозрюваного чи обвинуваченого копія постанови про порушення кримінальної справи вручається або надсилається на їх письмову вимогу протягом трьох діб з моменту надходження такої вимоги (ч. 3 та 4 ст. 98-2 КПК України).

Якщо представлених матеріалів для порушення кримінальної справи виявиться недостатньо, прокурор або слідчий вправі повернути їх з вказівкою про причини для проведення додаткової перевірки, або винести постанову про відмову в порушенні кримінальної справи (ст. 99 КПК України).

Коли в результаті перевірки заяви чи повідомлення, що надійшли, не буде встановлено підстав для порушення кримінальної справи, але в матеріалах перевірки міститимуться дані про наявність у діянні особи адміністративного або дисциплінарного проступку чи іншого порушення громадського порядку, прокурор вправі, відмовивши в порушенні кримінальної справи, надіслати заяву або повідомлення на розгляд громадської організації, службі у справах дітей, трудовому колективу або власнику підприємства, установи, організації чи уповноваженому ним органу для вжиття відповідних заходів впливу або передати матеріали для застосування в установленому порядку заходів адміністративного стягнення (ст. 99 КПК України).

Постанову слідчого про відмову в порушенні кримінальної справи може бути оскаржено відповідному прокуророві, а якщо таку постанову винесено прокурором – вищестоящому прокуророві. Скарга подається особою, інтересів якої вона стосується, або її представником протягом семи днів з дня одержання копії постанови.

Право на оскарження постанови прокурора і слідчого про відмову в порушенні кримінальної справи надано особі, інтересів якої вона стосується, а так само її представнику. Для цього до суду подається відповідна заява в порядку, передбаченому ст. 236-1 КПК України [3].

Детально описаний нами порядок порушення кримінальної справи є традиційним для практики слідчих органів. Втім він не прийнятний для випадків, коли є необхідність у проведенні слідчих дій до порушення кримінальної справи. Йдеться про положення ч. 2 ст.190 КПК, згідно з якими у невідкладних випадках дозволяється проводити огляд місця події «при наявності для того підстав», після чого негайно порушується кримінальна справа [4, 434]. Наведена законодавча норма, спрямована на запобігання втрати слідів та обстановки на місці події, що має ознаки злочину. У комп'ютерних злочинах часом це чи не єдиний спосіб отримання доказів протиправної діяльності особи. Між тим, саме ця норма КПК викликала жваву дискусію серед деяких вчених і практиків, результати якої зводяться до рекомендацій, а подекуди й імперативних вимог дозволити проведення до порушення кримінальної справи не лише огляду місця події, але й деяких судових експертиз, обшуків, допитів. Зрештою цей тиск приніс свої плоди, і законодавець дозволив у ч. 3 ст. 187 КПК «з метою запобігти злочину» накладати арешт на кореспонденцію та знімати інформацію з каналів зв'язку [4, 427; 5, 37].

На нашу думку, яка повністю збігається з позицією В. Г. Гончаренка та М. Є. Блудиліної, «такого роду дозволи є категорично неприпустимими як явища поліцейського розслідування і повинні бути вилучені з нормативних актів як незаконні принаймні з трьох причин.

*По-перше*, якщо для огляду місця події ситуація невідкладності його проведення в абсолютній більшості випадків є очевидною, а саме така процедура огляду є необхідною, то арешт на кореспонденцію і зняття інформації з каналів зв'язку за визначенням не можуть бути невідкладними, бо для їх здійснення необхідна постанова голови апеляційного суду або його заступника, яка приймається на погоджене з прокурором подання слідчого і після вивчення поданих матеріалів та з урахуванням пояснень слідчого і думки прокурора (ч. 4 ст. 187 КПК). Як видно, підготовка до проведення цих слідчих дій йде розмірено, ґрунтовно і відносно тривалий час, що цілком зрозуміло, бо йдеться про серйозні обмеження конституційних прав людини. В чому ж тоді полягає невідкладність?

*По-друге*, якщо зважити на те, що невідкладність пов'язується з необхідністю запобігти злочину (а саме це зазначено в ч. 4 ст. 187 КПК), то виявиться, що дана норма вступає в протиріччя зі ст. 4 КПК, яка передбачає обов'язок слідчого порушити кримінальну справу «в кожному випадку виявлення ознак злочину», не маючи на увазі порушення кримінальної справи для запобігання злочину. В такому разі проведення арешту кореспонденції або зняття інформації з каналів зв'язку до порушення кримінальної справи з метою запобігти злочину є повністю алогічним. Більше того, запобігання злочину і теоретично, і практично можливе у випадку виявлення умислу та на стадії готування до злочину, але виявлення умислу не розглядається як стадія вчинення злочину і не тягне за собою кримінальної відповідальності, а для визнання готування таким, що потребує порушення кримінальної справи, необхідно в силу ст. 2 КК України виявити ознаки злочину, до якого відбувається готування. Це означає, що слідчий повинен мати вже здобуту оперативним шляхом офіційну й достовірну інформацію про злочин, що готується, і відповідно на неї реагувати. Але ж запобігати злочинам, про готування до яких стає достовірно відомо, необхідно негайно, а не затівати слідчо-прокурорсько-суддівську процедуру одержання дозволу на зазначені акції. Тим більше, що правоохоронні органи на підставі відомих законодавчих актів за чітко встановленою процедурою мають можливість в інший спосіб одержувати необхідну для запобігання злочинам інформацію і реально на її підставі запобігати їм. Тому мотивація ст. 187 КПК про дозвіл слідчому накладати арешт на кореспонденцію та знімати інформацію з каналів зв'язку до порушення кримінальної справи з тим, щоб запобігти злочину, є фікцією, і цій нормі взагалі не місце в КПК.

*По-третє*, в ч. 3 ст. 187 КПК немає вказівки на те, що після «негайного» чи «невідкладного» прослуховування чи перлюстрації зразу ж повинна бути порушена кримінальна справа, що взагалі не є засобом сприяння розслідуванню (якого, до речі, ще немає), а узаконенням позапроцесуального і свавільного попраання прав громадян» [6, 48–53].

Що стосується питання про проведення огляду місця події до порушення кримінальної справи, дозволимо собі таке застереження. У випадках, коли слідчий у зв'язку з певними обставинами змушений без порушення кримінальної справи на проведення такого процесуального заходу як огляд, що має своїм спрямуванням виявлення, фіксацію, збирання й дослідження доказів, то від-

разу після проведення цієї слідчої дії неодмінно повинна бути винесена відповідна постанова про порушення кримінальної справи. На наше переконання, що ґрунтується на власному практичному досвіді, слідчий, приймаючи рішення про проведення повномасштабного огляду місця події, вже бачить ознаки злочину (інакше огляд не треба починати), а винесення постанови про порушення справи одразу після закінчення огляду є по суті формальною процедурою [7, 85].

Окрім розглянутого в нашій статті, потребують окремої уваги і відповідного унормування в чинному КПК питання про порушення кримінальної справи за матеріалами реалізації оперативних розробок, результатів оперативно-розшукових дій із виявлення злочинів, до проведення

яких уповноважені оперативні підрозділи долучають спеціалістів, обізнаних на питаннях певної галузі знань, у даному випадку – комп'ютерних технологіях. Йдеться про спеціальні дослідження, що проводяться на стадії порушення кримінальної справи або під час невідкладних слідчих дій, матеріали за результатами яких можуть бути доказами у кримінальній справі. Щоб виключити проблему з використанням таких матеріалів як доказів, пропонується внести зміни у редакцію ст. 65 КПК, якими передбачити, що «докази у кримінальній справі, крім іншого, встановлюються матеріалами спеціальних досліджень на стадії порушення кримінальної справи або під час проведення невідкладних слідчих дій».

### ВИКОРИСТАНІ ДЖЕРЕЛА

1. Вехов В. Б. Компьютерные преступления : способы совершения и раскрытия / В. Б. Вехов. – М. : Право и Закон, 1996. – 182 с.
2. Михеєнко М. М. Кримінальний процес України : підр. для юрид. вузів / М. М. Михеєнко, В. Т. Нор, В. П. Шибіко. – 2-ге вид., перероб. і доп. – К. : Либідь, 1999. – 534 с.
3. Кримінально-процесуальний кодекс України : наук.-практ. комент. / за заг. редакцією В. Т. Маляренка, В. Г. Гончаренка. – 5-те вид., переробл. – К. : Юрисконсульт, КНТ, 2008. – 896 с.
4. Кримінально-процесуальний кодекс України : наук.-практ. комент. / за заг. редакцією В. Т. Маляренка, В. Г. Гончаренка. – 6-те вид., переробл. та доповн. – К. : Юрисконсульт, Юстініан, 2010. – 896 с.
5. Нове у кримінально-процесуальному законодавстві України / За ред. Ю. М. Groшевого. – Харків : Право, 2002. – 160 с.
6. Гончаренко, В. Г. Правові питання порушення кримінальної справи / В. Г. Гончаренко, М. Є. Блудиліна // Вісник Академії адвокатури України. – 2010. – Число 2 (18). – С. 48-53.
7. Гончаренко, В. И. Гарантии соблюдения социалистической законности в предварительном следствии / В. И. Гончаренко // Юридические гарантии применения советских правовых норм и укрепления социалистической законности : тезисы докладов и сообщений (5-7 октября 1971 г.); Пятая секция. – К. : КГУ, 1971.

#### *Европіна І. В. Особенности возбуждения уголовных дел о компьютерных преступлениях*

В статье освещается порядок, поводы и основания возбуждения уголовных дел о преступлениях в сфере использования компьютеров, указываются и исследуются присущие этому особенности, анализируются проблемы.

**Ключевые слова:** расследование преступлений, следственная проверка, возбуждение дела, следы преступления, оперативно-розыскная деятельность, материалы специальных исследований

#### *Ievropina Iryna. The specifics of the beginning of criminal proceeding on cyber crimes*

The article deals with order and grounds of cyber crime proceedings and researches their distinctive features and problems.

**Key words:** investigation of crime, pretrial checking, beginning of case, tracks of crime, operative and search activity, materials of special research

### ПОДІЇ

## Наукова конференція «Україна. 20 років шляхом незалежності»

23 травня 2011 р. в Академії адвокатури України відбулась Міжнародна науково-практична конференція «Україна. 20 років незалежності». Доповіді викладачів з різних юридичних ВНЗ були присвячені проведенню правових реформ в незалежній Україні та визначну роль вузівської науки у становленні і розвитку національного законодавства. Професор З. В. Ромовська назвала свою доповідь «Творчість Івана Франка як дзеркало сучасних проблем України». Особливості формування господарського законодавства України на сучасному етапі узагальнив професор Національної академії управління Р. Б. Прилуцький. Декілька доповідей були присвячені важливим питанням застосування земельного законодавства. Зокрема доцент Національного університету біоресурсів і права України імені академіка В. З. Янчука Ю. С. Петлюк висвітлив правові аспекти здійснення моніторингу земель в Україні, а доцент Академії адвокатури України О. М. Ковтун зосередила увагу на правовому регулюванні програмування використання та охорони земель в Україні. Всі доповідачі засвідчили, що Україна впевнено крокує шляхом демократизації законодавства, його оновлення, приведення у відповідність зі світовими стандартами.

За матеріалами офіційного сайту Академії адвокатури України <http://aau.edu.ua>