1. *Д'яконова І. І.* Теоретико-методологічні основи функціонування банківської системи України: монографія / І. І. Д'яконова. — Суми: ВТД «Університетська книга», 2007. — 400 с.
2. *Безклубий І. А.* Теоретичні проблеми банківських правочинів: автореф. дис. … доктора юрид. наук: спец. 12.00.03 / І. А. Безклубий; Київ. нац. ун-т ім. Т. Шевченка. — К., 2006. — 32 с.
3. *Лепех С. М.* Кредитний договір: автореф. дис. … канд. юрид. наук: спец. 12.00.03 / С. М. Лепех ; Львів. нац. ун-т ім. І. Франка. — Л., 2004. — 19 с.
4. *Іваненко Л. М.* Правові засади споживчого кредитування / Л. М. Іваненко // Вісник КНТЕУ. — 2011. — № 1. — С. 103–110.
5. *Шемшученко Г. Ю.* Фінансово-правове регулювання банківського кредитування: монографія / Г. Ю. Шемшученко. — К.: ТОВ «Видавництво «Юридична думка», 2006. — 264 с.
6. *Баришніков А. Г.* Адміністративно-правове регулювання сфери банківського кредитування в Україні: автореф. дис. … канд. юрид. наук за спец.: 12.00.07 / А. Г. Баришніков. — Запоріжжя, 2009. — 20 с.
7. *Владичин У. В.* Банківське кредитування: навч. посіб. / За ред. д.е.н., проф. С. К. Реверчука. — К.: Атіка, 2008. — 648 с.
8. *Вітка Ю. В.* Правове регулювання споживчого кредиту: стан та перспективи / Ю. В. Вітка // Фінанси України. — 2013. — № 10. — С. 75–86.
9. *Про фінансові послуги та державне регулювання ринків фінансових послуг:* Закон України від 12.07.2001 р. № 2664-III // Відомості Верховної Ради України (ВВР). — 2002. — № 1. — Ст. 1.
10. *Про банки і банківську діяльність:* Закон України від 07.12.2000 р. № 2121-III // Відомості Верховної Ради України (ВВР). — 2001. — № 5–6. — Ст. 30.
11. *Про затвердження Правил надання банками України інформації споживачу про умови кредитування та сукупну вартість кредиту:* Постанова Правління Національного банку України від 10.05.2007 р. № 168 // Офіційний вісник України. — 2007. — № 39. — Ст. 1569. — Код акту 39884/2007.
12. Т*орубка Л. В.* Споживче кредитування в Україні: сучасний стан і напрями розвитку / Л. В. Торубка // Вісник Університету банківської справи НБУ. — 2011. — № 3(12). — С. 227–230.
13. *Про затвердження Положення про порядок ведення реєстру комерційних агентів (комерційних представників) банків:* Постанова Правління Національного банку України від 20.09.2012 р. № 386 // Офіційний вісник України. — 2012. — № 80. — Ст. 3228. — Код акту 63886/2012.
14. *Про захист прав споживачів:* Закон України від 12.05.1991 р. № 1023-XII // Відомості Верховної Ради УРСР (ВВР). — 1991. — № 30. — Ст. 379.
15. *Про організацію формування та обігу кредитних історій:* Закон України від 23.06.2005 р. № 2704-IV // Відомості Верховної Ради України (ВВР). — 2005. — № 32. — Ст. 421.

О. М. Моїсєєв
зав. кафедри кримінального права і процесу
Донецького національного університету,
д-р юрид. наук, професор

ІНФОРМАЦІЙНА БЕЗПЕКА ДОПИТУ ЕКСПЕРТА У РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ

Ключові слова: процесуальні дії, дистанційне судове провадження, допит експерта, режим відеоконференції, інформаційна безпека.

Сучасне суспільство рухається шляхом активного розвитку інформаційно-комунікаційних технологій. Інформатизація охоплює всі основні сфери життя

суспільства, відтак і розвиток вітчизняного законодавства набуває нових тенденцій. Зокрема, однією з новел, запроваджених Кримінальним процесуальним кодексом України 2012 року, стало використання відеоконференцзв'язку під час досудового та судового провадження у кримінальній справі. Утім не втрачають актуальності проблеми комунікативної взаємодії експерта з учасниками кримінального провадження в дистанційній формі. До того ж, запровадивши таку новацію, законодавець залишив невирішеними низку питань, одним із яких є забезпечення інформаційної безпеки під час допиту особи в режимі відеоконференції.

Таким чином, у ст. 1 Закону України «Про судову експертизу» зміст поняття «судова експертиза» визначено як дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів дізнання, досудового і судового слідства [1]. За результатами проведення зазначеного дослідження експерт складає висновок, що є одним із передбачених Кримінальним процесуальним кодексом джерел доказів.

Такі науковці як Т. В. Авер'янова [2], А. І. Вінберг [3], О. О. Ейсман [4], Н. І. Клименко [5], В. Я. Колдін [6], М. Я. Сегай [7], В. Ю. Шепітько [8], О. Р. Шляхов [9] та ін. у своїх працях приділили багато уваги дослідженню висновку експерта. Однак у світлі активного розвитку інформаційних технологій не отримало розв'язання питання забезпечення інформаційної безпеки під час дистанційного досудового розслідування та судового провадження.

Отже, метою статті вважаємо дослідження проблем забезпечення інформаційної безпеки під час допиту експерта у режимі відеоконференції та розроблення відповідних рекомендацій для суб'єктів кримінального провадження, які забезпечують процес дистанційного допиту.

У літературі наукового спрямування висловлено пропозицію щодо розширення положень статей 232 та 336 Кримінального процесуального кодексу нормою щодо участі експерта в досудовому та судовому провадженні у режимі відеоконференцзв'язку. Також доведено, що така взаємодія експерта з іншими учасниками кримінального провадження не тільки сприятиме скороченню витрат на відрядження для судового експерта й дозволить мінімізувати відволікання його від основної роботи, а й значною мірою підвищить ефективність проведення експертизи в судовому засіданні та допиту експерта стосовно проведеного ним дослідження. Для впровадження змін до положень указаних статей авторами висловлено рекомендацію відносно доцільності обладнання спеціальних кімнат для проведення відеоконференцій не тільки в судах, а й у державних експертних установах, відповідальність за функціонування яких необхідно покласти на керівників цих установ [10].

Звертаючись безпосередньо до Кримінального процесуального кодексу, бачимо, що, згідно з п. 3 ст. 232 КПК України, використання у дистанційному досудовому розслідуванні технічних засобів і технологій повинно гарантувати належну якість зображення і звуку, а також інформаційну безпеку. Учасникам слідчої (розшукової) дії має бути забезпе-чено можливість ставити запитання і отримувати відповіді осіб, які беруть участь у слідчій (розшуковій) дії дистанційно, реалізовувати інші надані їм процесуальні права та виконувати процесуальні обов'язки, передбачені КПК [11]. Викликає сумнів можливість стовідсоткового забезпечення якості зображення і звуку, а також інформаційної безпеки, оскільки створення та роботу технічних пристроїв зв'язку забезпечують конкретні працівники, до того ж використання таких пристроїв пов'язане з технічними складнощами в плані передавання інформації (наявність шумів),

які зумовлюють специфіку процесів відображення (тобто передавання та отримання) інформації, властиву конкретним пристроям зв'язку.

Позаяк вітчизняне законодавство впевнено наближається до стандартів європейських країн, вважаємо доречним розгляд поняття інформаційної безпеки з позиції країн Європейського Союзу, де питання забезпечення інформаційної безпеки суспільства незмінно перебувають у центрі уваги.

Усе більшого збитку підприємницькій діяльності громадян і організацій, а також діяльності державних органів завдає поширення в комп'ютерних мережах шкідливих програм, здійснення несанкціонованого доступу до інформаційних ресурсів, поширення «інформаційної» макулатури (спаму).

Розширюється застосування сучасних інформаційних технологій для вчинення злочинних діянь у сфері порушення конституційних прав і свобод людини й громадянина, ведення економічного та промислового шпигунства, розкриття відомостей, що становлять особисту, сімейну, комерційну, державну та інші охоронювані законом таємниці.

Посилюється небезпека використання сучасних інформаційних технологій для завдання збитку політичним, економічним, військовим чи іншим інтересам держави з боку терористичних організацій і ворожих держав [12, с. 14].

Усе це переконливо свідчить, що метою створення системи забезпечення безпеки інформаційних технологій є запобігання або мінімізація збитку (прямого чи непрямого, матеріального, морального або іншого), якого зазнають суб'єкти інформаційних відносин від небажаного впливу на інформацію, її носії та процеси обробки.

Забезпечення інформаційної безпеки характеризується діяльністю щодо недопущення шкоди властивостям об'єкта безпеки, зумовленим інформацією та інформаційною інфраструктурою, а також засобами та суб'єктами цієї діяльності [12, с. 37].

Розглянемо детальніше критерії інформаційної безпеки, якими є:

1) доступність (інформація відкрита для доступу, і засоби її передавання функціонують, незважаючи на можливі негативні події, наприклад, вимкнення електроживлення, стихійні лиха, нещасні випадки або напади);

2) аутентифікація (підтвердження заявленої ідентичності юридичних осіб або користувачів);

3) цілісність (підтвердження, що інформація, яку було надіслано, отримано або збережено, є цілою і незмінною);

4) конфіденційність (захист повідомлень або збереженої інформації від несанкціонованого перехоплення і перегляду [13, с. 94]).

Інформаційні загрози реалізуються у вигляді: 1) порушення адресності і своєчасності інформаційного обміну, протизаконного збору та використання інформації; 2) здійснення несанкціонованого доступу до інформаційних ресурсів та їх протиправного використання; 3) розкрадання інформаційних ресурсів із банків і баз даних; 4) порушення технології обробки інформації [14, с. 20].

Політика ж Європейського Союзу у сфері забезпечення інформаційної безпеки грунтується на таких складових:

1) забезпечення прикладного характеру правових норм на основі загального розуміння основних питань інформаційної безпеки і спеціальних заходів її забезпечення;

2) необхідність постійного вдосконалення правового регулювання з урахуванням технічного прогресу і породжуваних ним нових загроз;

3) потреба в доповненні ринкових механізмів політичними заходами;

4) формування європейського внутрішнього ринку інформаційно-комунікаційних послуг [13, с. 94].

Важливим нормативно-правовим актом, ухваленим у сфері забезпечення інформаційної безпеки, є Рекомендації Комісії Європейських Співтовариств 94/820/ЕС від 19 жовтня 1994 року, що стосуються правових аспектів електронного обміну даними [15]. Електронний обмін даними — це міжкомп'ютерний обмін діловими, комерційними та фінансовими електронними документами, наприклад: замовленнями, платіжними інструкціями, контрактними пропозиціями, накладними, квитанціями [16, с. 60].

Згідно з цими рекомендаціями, всі економічні суб'єкти і організації, що здійснюють свою торговельну діяльність із використанням електронного обміну даними, повинні спиратися на Європейську типову угоду про електронний обмін даними. Особливу увагу приділено питанням безпеки повідомлень електронного обміну даними, зокрема процедурам і заходам безпеки від ризиків несанкціонованого доступу, змінення, затримки, знищення або втрати інформації, конфіденційності та захисту персональних даних.

Для забезпечення захисту інформації від несанкціонованого доступу учасники кримінального провадження мають дотримуватися основних принципів захисту інформації:

1) принципу обгрунтованості доступу, який полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню «форму допуску» для отримання інформації необхідного йому рівня конфіденційності, водночас означена інформація необхідна йому для виконання його процесуальних функцій;

2) принципу достатньої глибини контролю доступу, за яким засоби захисту інформації повинні містити механізми контролю доступу до всіх видів інформаційних і програмних ресурсів автоматизованих систем, які за принципом обгрунтованості доступу слід розподіляти між користувачами;

3) принципу розмежування потоків інформації, відповідно до якого для убезпечення від порушення безпеки інформації, що, наприклад, може статися в момент запису секретної інформації на несекретні носії та в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також у процесі передачі секретної інформації незахищеними каналами і лініями зв'язку, — а отже необхідно здійснювати відповідне розмежування потоків інформації;

4) принципу чистоти повторно використовуваних ресурсів, який полягає в очищенні ресурсів, що містять конфіденційну інформацію, під час їх видалення або звільнення користувачем до перерозподілу цих ресурсів іншим користувачам;

5) принципу персональної відповідальності, згідно з яким кожен користувач повинен нести персональну відповідальність за свою діяльність у системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, тобто будь-які випадкові чи навмисні дії, які призводять або можуть призвести до несанкціонованого ознайомлення з конфіденційною інформацією, її викривлення чи знищення, або ж роблять таку інформацію недоступною для законних користувачів;

6) принципу цілісності засобів захисту, яким передбачено, що засоби захисту інформації в автоматизованих системах повинні точно виконувати свої функції відповідно до названих принципів і бути ізольованими від користувачів, а також обладнаними спеціальним захищеним інтерфейсом для засобів контролю, сигналізації про спроби порушення захисту інформації та впливу на процеси в системі [14, с. 35–36].

В Європейському Союзі до основних заходів протидії загрозам інформаційної безпеки відносять:

1) підвищення обізнаності, що передбачає проведення інформаційних та освітніх кампаній і обмін передовим досвідом у розглядуваній сфері;

2) запровадження Європейської системи попередження та інформування;

3) забезпечення технологічної підтримки, пов'язаної зі стратегією розвитку системи інформаційної безпеки;

4) забезпечення ринково орієнтованих способів стандартизації та сертифікації;

5) забезпечення безпеки в урядових установах;

6) міжнародна взаємодія, що передбачає як розширення діалогу між державами-учасниками з приводу підвищення ефективності забезпечення інформаційної безпеки підприємництва [13, с. 96–97].

Звертаючись до дослідження проблем забезпечення інформаційної безпеки під час допиту експерта у режимі відеоконференції важливо зазначити, що допит є одним із засобів пізнання слідчим (судом) подій, фактів і обставин, які він не сприймав безпосередньо, шляхом сприйняття свідчень осіб про ці факти, обставини, події. Основне в допиті — інформація, основні психологічні особливості якої є такими: 1) під час допиту допитуваний розв'язує цілу низку розумових завдань, постановлених слідчим (судом) та ним самим; 2) вербальне передавання інформації пов'язане з наявністю бажання, інтересу, потреби передати слідчому (суду) опис подій; 3) у процесі допиту допитуваний викладає не власне сприйняття, а лише спогад, враження про нього; 4) в ході допиту свідка, підозрюваного, обвинуваченого у всіх випадках із боку слідчого (суду) потрібна активна розумова діяльність; для забезпечення високої психічної активності допитуваного необхідно викликати і підтримувати у нього відповідний емоційний стан [17, с. 6]. Інакше кажучи, формування показань як комплекс складних психологічних процесів відбувається за активної участі особи допитуваного. Тому важливими умовами проведення дистанційного допиту, безумовно, є забезпечення належної якості зображення і звуку. З цією метою слідчий, прокурор чи слідчий суддя повинні залучити до участі у проведенні слідчої дії в режимі відеоконференції фахівця, який має спеціальні знання та навички застосування відповідних технічних засобів і технологій.

Проведення відеоконференції має передбачати забезпечення інформаційної безпеки, тобто необхідно гарантувати захищеність інформації та інфраструктури, що її підтримує від випадкового або навмисного впливу природного чи штучного характеру, що може завдати шкоди кримінальному провадженню, призвести до розкриття таємниці досудового розслідування, змісту показань, наданих під час слідчої дії, даних про осіб, які перебувають під державним захистом, тощо [18].

Підсумовуючи викладене, вважаємо, що подальший розвиток сучасного кримінального процесуального законодавства потребує нормативно-правового закріплення загальної стратегії забезпечення інформаційної безпеки слідчих та судових дій, які проводяться у дистанційному режимі. На особливу увагу заслуговує розроблення процедури поводження з інформацією, зберігання інформації, захисту цієї інформації від недозволеного розкриття або неправомірного використання.

---

1. *Про судову експертизу :* Закон України від 25 лютого 1994 р. № 4038-XII // Відомості Верховної Ради України. — 1994. — № 28. — Ст. 23.

2. *Аверьянова Т. В.* Судебная экспертиза: Курс общей теории [Текст] / Т. В. Аверьянова. — М.: Норма, 2006. — 480 с.

3. *Винберг А. И.* Основные принципы советской криминалистической экспертизы [Текст] : монография / А. И. Винберг — М. : Госюриздат, 1949. — 132 с.
4. *Эйсман А. А.* Заключение эксперта. Структура и научное обоснование [Текст] / А. А. Эйсман. — М. : Юрид. лит., 1967. — 152 с.
5. *Клименко Н. І.* Судова експертологія : курс лекцій [Текст] / Н. І. Клименко. — К. : Видавничий дім «Ін Юре», 2007. — 528 с.
6. *Колдин В. Я.* Судебно-экспертные науки и технологии [Текст] / В. Я. Колдин, О. А. Крестовников // Теория и практика судебной экспертизы. — М. : МЮ РФ, 2006. — № 1. — С. 12–19.
7. *Сегай М. Я.* Судебная экспертология: концептуальные основы экспертной методологии [Текст] / М. Я. Сегай // Теорія та практика судової експертизи і криміналістики. Випуск 2 : збірник матеріалів міжнарод. наук.-практ. конф. / Міністерство юстиції України, Харківський науково-дослідний інститут імені засл. проф. М. С. Бокаріуса, Академія правових наук України, Національна юридична академія України ім. Ярослава Мудрого; [ред. колегія : М. Л. Цимбал, М. І. Панов, Е. Б. Сімакова-Єфремян та ін.] — Харків : Право, 2002. — С. 36–42.
8. *Шепітько В. Ю.* Проблеми використання спеціальних знань крізь призму сучасного кримінального судочинства в Україні / В. Ю. Шепітько // Судова експертиза. — 2014. — № 1. — С. 11-18.
9. *Шляхов А. Р.* Судебная экспертиза: организация и проведение [Текст] / А. Р. Шляхов. — М.: Юрайт, 2001. — 187 с.
10. *Моїсєєв О. М.* Експериментальне вивчення дистанційної форми допиту судового експерта / О. М. Моїсєєв, О. А. Лєгостаєв // Правничий часопис Донецького університету. — 2013. — № 1(29). — С. 174–181.
11. *Кримінальний процесуальний кодекс України від 13 квіт. 2012 р.* // Офіційний вісник України. — 2012. — № 37. — 25 трав. — Ст. 1370.
12. *Организационно-правовое обеспечение информационной безопасности :* учебн. пос. [для студентов высш. учеб. завед.] / А. А. Стрельцов [и др.]; под ред. А. А. Стрельцова. — М. : Изд. центр «Академия», 2008. — 256 с.
13. *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза : монография / А. А. Смирнов. — М. : ЮНИТИ-ДАНА, 2011. — 196 с. [Электронный ресурс]. — Режим доступа: http://spkurdyumov.narod.ru/smirnov.pdf.
14. *Малюк А. А.* Введение в защиту информации в автоматизированных системах / Малюк А. А., Пазизин С. В., Погожин Н. С. — М. : Горячая линия-Телеком, 2001. — 148 с.
15. *Commission Recommendation 94/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange* // Official Journal of the European Communities. — 1994. — L 338. — P. 0098-0117.
16. *Волик О. Ф.* Митні інформаційні технології : навч. посіб. / Волик О. Ф., Кащева О. В.; за ред. П. В. Пашка. — К. : Знання, 2011. — 391 с.
17. *Коновалова В. Е.* Психология в расследовании преступлений / В. Е. Коновалова. — Х. : Вища школа, 1978. — 143 с.
18. *Кримінальний процесуальний кодекс України:* Науково-практичний коментар : у 2 т. / О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль [та ін.; за заг. ред. Тація В. Я., Пшонки В. П., Портнова А. В.]. — Х. : Право, 2012. — Т. 1. — 2012. — 768 с.