Ученые записки Таврического национального университета им. В. И. Вернадского
Серия «Юридические науки». Том 27 (66). 2014. № 4. С. 184-189.

УДК 343.98

ІНФОРМАЦІЙНА БЕЗПЕКА ДОПИТУ ЕКСПЕРТА В РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ

Моїсєєв О. М.

Донецький національний університет,
м. Донецьк, Україна

Досліджено проблему забезпечення інформаційної безпеки під час допиту судового експерта в режимі відеоконференції. Доведено доцільність розроблення та нормативно-правового закріплення загальної стратегії забезпечення інформаційної безпеки процесуальних дій, які проводяться в дистанційному режимі.

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, а отже, 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 в кримінальній справі. Проте не втрачають актуальності проблеми комунікативної взаємодії експерта з учасниками кримінального провадження в дистанційній формі. Крім того, запровадивши таку новацію, законодавець залишив не вирішеними 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 в провадженні органів дізнання, досудового й судового слідства [1]. За результатами проведення зазначеного дослідження експерт складає висновок, що є одним із передбачених Кримінальним процесуальним кодексом України 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 інші 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* цієї роботи вважаємо дослідження проблем забезпечення інформаційної безпеки під час допиту експерта в 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 України нормою щодо участі експерта в досудовому та судовому провадженні в 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 щодо 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 України (далі – КПК України), бачимо, що згідно з п. 3 ст. 232 КПК України використання в дистанційному досудовому розслідуванні технічних засобів і технологій повинно гарантувати належну якість зображення й звуку, а також інформаційну безпеку. Учасникам слідчої (розшукової) дії має бути забезпечено можливість ставити запитання й отримувати відповіді осіб, які беруть участь у слідчій (розшуковій) дії дистанційно, реалізовувати інші надані їм процесуальні права та виконувати процесуальні обов'язки, передбачені КПК України [11]. Викликає сумнів можливість стовідсоткового забезпечення якості зображення й 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.

Оскільки 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 такі:

1) доступність означає, що інформація відкрита для доступу, а засоби її передавання функціонують, незважаючи на такі можливі негативні події, як 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 й перегляду [13, с. 94].

Інформаційні загрози реалізуються у такому вигляді: 1) порушення адресності та 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 ґрунтується на таких складових:

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

2) необхідність постійного вдосконалення правового регулювання з урахуванням технічного прогресу та зумовлюваних 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 із цими рекомендаціями всі економічні суб'єкти й 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, а саме:

1) принципу обґрунтованості 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 обґрунтованості доступу слід розподіляти між користувачами;

3) принципу розмежування потоків інформації, відповідно до якого для убезпечення від порушення безпеки інформації, що може статися в момент запису секретної інформації на несекретні носії та в несекретні файли, її передачі програмам і процесам, непризначеним 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].

У Європейському Союзі до основних заходів протидії загрозам інформаційної безпеки відносять такі:

1) підвищення обізнаності, що передбачає проведення інформаційних та освітніх кампаній та 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 в режимі відео конференції, важливо зазначити, що допит є одним із засобів пізнання слідчим (судом) подій, фактів й 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) у ході допиту свідка, підозрюваного, обвинуваченого у всіх випадках із боку слідчого (суду) потрібна активна розумова діяльність; для забезпечення високої психічної активності допитуваного необхідно викликати й підтримувати в 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 є забезпечення належної якості зображення та звуку. З цією метою слідчий, прокурор чи слідчий суддя повинні залучити до участі в 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 в дистанційному режимі. На особливу увагу заслуговує розроблення процедури поводження з інформацією, зберігання інформації, захисту цієї інформації від недозволеного розкриття або неправомірного використання.

Список літератури:

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 / Т.В. Аверьянова. – М. : Норма, 2006. – 480 с.

3. Винберг А.И. Основные принципы советской криминалистической экспертизы : [монография] / А.И. Винберг – М. : Госюриздат, 1949. – 132 с.

4. Эйсман А.А. Заключение эксперта. Структура и научное обоснование / А.А. Эйсман. – М. : Юрид. лит., 1967. – 152 с.

5.Клименко Н.І. Судова експертологія : [курс лекцій] / Н.І. Клименко. – К. : Видавничий дім «Ін Юре», 2007. – 528 с.

6. Колдин В.Я. Судебно-экспертные науки и технологи / 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 / М.Я. Сегай // Теорія та практика судової експертизи і криміналістики : збірник матеріалів міжнарод. наук.-практ. конф. / ред. колегія: М.Л. Цимбал, М.І. Панов, Е.Б. Сімакова-Єфремян та ін. – Вип. 2. – Х. : 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 / 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 квітня 2012 р. // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.
12. Организационно-правовое обеспечение информационной безопасности : [учеб. пос. для студентов высш. учеб. завед.] / [А.А. Стрельцов и др.] ; под ред. А.А. Стрельцова. – М. : Изда. 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. – [Електронний ресурс]. – Режим доступу : http://spkurdyumov.narod.ru/ smirnov.pdf.
14. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – 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.] / [О.Ф. Волик, О.В.Кащева] ; 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. В.Я. Тація, В.П. Пшонки, А.В. Портнова. – Х. : Право, 2012. – Т. 1. – 2012. – 768 с.

Моисеев А. М. Информационная безопасность допроса эксперта в режиме видеоконференции / А. М. Моисеев // Ученые записки Таврического национального университета имени В. И. Вернадского. Серия: Юридические науки. – 2014. – Т. 27 (66). № 4. – С. 1184-189.

Исследована проблема обеспечения информационной безопасности при допросе судебного эксперта в режиме видеоконференции. Доказана целесообразность разработки и нормативно-правового закрепления общей стратегии обеспечения информационной безопасности процессуальных действий, которые проводятся в дистанционном режиме.

Ключевые слова: процессуальные действия, дистанционные судебное производство, допрос эксперта, режим видеоконференции, информационная безопасность.

THE PROVIDING OF INFORMATION SECURITY DURING INTERROGATION OF EXPERT IN THE MODE OF VIDEOCONFERENCE

Moiseev A. M.
Donetsk National University,
Donetsk, Ukraine

The problem of information security during remote prejudicial investigation and court proceedings is investigated. The suggestion for implementing of interrogation of expert in the mode of videoconferenceis founded. The legal basis of the proceedings in the remote form is considered. It is found that, in accordance with Section 3, Article. 232 of Code of Criminal Procedure, the use of technical means and technologies in remote prejudicial investigation should provide the necessary quality of picture and sound, as well as information security. Remote form of interaction will help to reduce the costs of business trips for a court expert. Also reduced the gap expert from operations and greatly enhance the efficiency of the examination in the hearing and questioning the effectiveness of an expert on the examination conducted. The expediency of development and regulatory consolidation of the common strategy of proceedings information security providing, which are conducted remotely, is proved. It is recommended to equip the special offices in the state forensic institutions for video conferencing in court. Responsible for the operation of such offices should be entrusted to the heads of expert institutions. These guarantees mean information security and infrastructure that supports it from accidental or intentional exposure to natural or artificial nature that may harm the criminal proceedings, to result in the disclosure of the secrets of pre-trial investigation, the content of the testimony given during the investigative actions, data on persons who are under state protection, and so on. In addition, the detailed regulation requires careful handling procedures with information, its savings and protection against unauthorized or irregular use.

Key words: legal proceedings, remote judicial proceedings, interrogation of expert, mode of videoconference, information security.