УДК 343.98

Бєжанова А.В.
адвокат, викладач першої категорії
Харківський автомобільно-дорожній технікум

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ У ДИСТАНЦІЙНОМУ КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Постановка проблеми. Стрімке вдосконалення технічних характеристик різних засобів зв'язку як невід'ємний фактор поступового вступу суспільства в епоху інформаційного простору зумовлює не лише динамічну появу нових технічних можливостей для перехоплення та копіювання інформації, переданої за допомогою технічних каналів зв'язку, а й необхідність у перегляді процесуального та тактико-криміналістичного потенціалу даної інформації як доказу в кримінальному судочинстві. В сучасних умовах інформатизація охоплює всі основні сфери життя суспільства, зокрема запровадження та використання відеоконференції під час досудового розслідування та судового розгляду в кримінальному провадженні.

З огляду на викладене одним із головних аспектів удосконалення діяльності правоохоронних та судових органів є визначення шляхів і засобів забезпечення інформаційної безпеки під час використання технічних засобів і технологій у дистанційному кримінальному провадженні. Це свідчить про актуальність дослідження можливостей ефективного використання науково-технічних досягнень у кримінально-процесуальній діяльності.

Огляд останніх досліджень і публікацій. проблематика науково-технічного забезпечення процесу розкриття та розслідування злочинів для кримінально-процесуального права не є новою. Дослідження технічного забезпечення розслідування кримінальних правопорушень висвітлені у наукових працях В.П. Бахіна, Р.С. Бєлкіна, В.В. Бірюкова, Г.І. Грамовича, І.А. Ієрусалимова, А.В. Іщенка, Н.С. Карпова, М.І. Клименка, В.В. Коваленка, В.С. Кузьмічова, М.В. Салтевського, Л.Д. Удалової, С.А. Шейфера, В.Ю. Шепітька та інших вчених. Відзначимо, що вказані вчені розглядали використання технічних засобів переважно як засоби фіксації ходу та результатів проведення процесуальних дій. Можливості проведення слідчих дій і судового розгляду кримінального провадження в режимі віддаленого доступу за допомогою телекомунікаційних технологій відеоконференції у своїх роботах досліджували М.І. Бортун, Т.В. Деменко, І.В. Казначей, С.О. Книженко, Т.В. Михальчук, С.О. Новікова, І.В. Черниченко, М.В. Чижов, Д.О. Шингарьов. Проте не втрачають актуальності проблеми забезпечення інформаційної безпеки під час використання технічних засобів і технологій у дистанційному кримінальному провадженні.

Формулювання завдання дослідження. Аналіз наукових досліджень свідчить, що вчені-криміналісти та процесуалісти у наукових публікаціях розглядають важливі аспекти науково-технічного забезпечення кримінального провадження з огляду на конкретні завдання, які стоять перед наукою. Проте проблематика забезпечення інформаційної безпеки під час використання технічних засобів і технологій у дистанційному кримінальному провадженні комплексно не розглядалась і відповідної наукової розробки не отримала. Наукового дослідження потребують правові підстави застосування технічних засобів і технологій у дистанційному кримінальному

провадженні, межі допустимості та порядок їх використання у кримінальному провадженні, а також питання надання юридичної сили відомостям, отриманим шляхом застосування режиму відеоконференції.

Виклад основного матеріалу. Кримінальний процесуальний кодекс України (далі – КПК України) згідно з п. 3 ст. 232 передбачає використання у дистанційному досудовому розслідуванні та судовому провадженні технічних засобів і технологій, які мають забезпечувати належну якість зображення і звуку, дотримання принципу гласності та відкритості судового провадження, а також інформаційну безпеку. Учасникам кримінального провадження повинна бути забезпечена можливість чути та бачити хід судового провадження, ставити питання і отримувати відповіді, реалізовувати інші надані їм процесуальні права та виконувати їх процесуальні обов'язки, передбачені КПК України [1]. Хід і результати процесуальних дій, проведених у режимі відеоконференції, фіксуються за допомогою технічних засобів відеозапису [2, с. 173–174]. Однак, як зазначає О.М. Моїсєєв, викликає сумнів можливість стовідсоткового забезпечення якості зображення й звуку, а також інформаційної безпеки, оскільки створення та роботу технічних пристроїв зв'язку забезпечують конкретні працівники, а 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 [3, с. 185]. На практиці проведення відеоконференції забезпечується за допомогою комп'ютерної техніки та Інтернету. Наприклад, ноутбук із вбудованою відеокамерою та можливістю відеозапису може бути використаний для проведення дистанційного провадження. З огляду на це виникає низка запитань щодо використання програмного забезпечення, наприклад, чи створюються такі програми спеціально для проведення дистанційного досудового (судового) розслідування або можна використати звичний для всіх скайп. Окрім того, постає й питання про те, які протоколи доступу використовувати (загальні чи спеціально виділену лінію для правоохоронних органів). Інтернет не є гарантованим та безпечним каналом передачі аудіо- та відеоданих. З цього приводу слушним є зауваження С.О. Книженко та Т.В.Деменко, що правоохоронні органи необхідно забезпечити окремою лінією зв'язку та спеціальним програмним забезпеченням, що дозволить гарантувати інформаційну безпеку під час проведення допиту в режимі відеоконференції [4, с. 209].

Відеоконференція (англ. videoconference) є галуззю інформаційної технології, що забезпечує одночасну двосторонню передачу, обробку, перетворення та подання інтерактивної інформації на відстань в реальному режимі часу за допомогою апаратно-програмних засобів обчислювальної техніки [5, с. 54]. У літературних джерелах відеоконференцію визначають також як телекомунікаційну технологію інтерактивної взаємодії двох і більше віддалених абонентів, за якої між ними можливий обмін аудіо- та відеоданими в реальному масштабі часу з урахуванням передачі керуючих даних [6, с. 65].

Одним з пріоритетних напрямків застосування систем відеоконференції сьогодні є забезпечення їх надійності. У кримінально-процесуальному судочинстві під час застосування режиму відеоконференції важливим є підтримання заданих параметрів якості. Будь-які спотворення можуть призвести до неправильного трактування інформації, а отже, до помилкових дій учасників відеоконференції.

Складність забезпечення надійності технічних засобів і технологій, які використовуються у дистанційному кримінальному провадженні, пов'язана з необхідністю підтримання високої швидкості обробки інформації і передачі даних з мінімальними затримками, а також з високою роздільною

здатністю зображення і якості звуку. Сучасні системи повинні володіти додатковим інструментарієм інтерактивної взаємодії. Варіанти вирішення цього питання не зовсім сумісні між собою, оскільки виробники не зацікавлені в інтеграції різних систем, а навпаки, система відеоконференції найчастіше є єдиним цілим з програмних і апаратних компонентів. Масштабувати таку систему можливо лише із застосуванням компонентів того ж виробника. Проте такий підхід є надмірно коштовним, а виділення коштів на використання таких технічних засобів державою не заплановано. Одним з перспективних шляхів вирішення проблеми забезпечення надійності відеоконференції є використання технологій розподілу навантаження мережі. Оптимальний розподіл мережевого навантаження дозволяє забезпечувати задані характеристики відеоконференції за рахунок керування інформаційними потоками [7].

Метою створення системи забезпечення безпеки інформаційних технологій є запобігання або мінімізація збитку, 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 [8, с. 37]. Проте в умовах сучасного стану злочинності забезпечити інформаційну безпеку органами Національної поліції неможливо лише на основі застосування захисних засобів і механізмів. У цих умовах, як зазначає І.К. Сезонова, необхідно вести активні наступальні (бойові) дії з використанням усіх видів інформаційної зброї та інших наступальних засобів з метою забезпечення переваги над злочинністю в інформаційній сфері [9, с. 413].

Натепер засоби захисту інформації представлені засобами зарубіжного виробництва. Це містить певну загрозу за умови використання таких систем в державних установах [10, с. 180]. Найчастіше у практичній діяльності застосовуються різні додатки для проведення відеоконференцій через глобальні телекомунікаційні мережі [11].

Основними методами підвищення надійності систем застосування режиму відеоконференції сьогодні є такі:

1) використання оптимізованих сучасних протоколів маршрутизації для оптимального і раціонального використання канального ресурсу системи;

2) використання алгоритмів децентралізованих систем та мереж, що самоорганізуються, які дозволяють розподілити навантаження на всі елементи пропорційно до ресурсів та характеристик, збільшуючи масштабованість та зменшуючи вартість такого рішення за відсутності необхідності підтримки протоколів прикладного рівня на мережевому обладнанні [12, с. 35];

3) застосування механізмів динамічного перерозподілу швидкості передачі інформації під час спільного обслуговування трафіку сервісів реального часу і трафіку даних, що допускає затримку [13, с. 64];

4) автоматичний спосіб визначення особи, що говорить в умовах реального часу, для надання потокам її мультимедійних даних найбільшого пріоритету під час передачі іншим учасникам [14, с. 149].

Основним способом управління навантаженням для організації надійності застосування режиму відеоконференції є забезпечення мінімальної швидкості передачі даних та максимальної швидкості обробки аудіо- та відеопотоку. Для вирішення цих проблем розроблені кодеки, що дозволяють стискати сигнал і кодувати його для каналу зв'язку, а також відновлювати і декодувати на стороні, що приймає [7].

Кодек (термінальний пристрій), який необхідний для організації надійного сеансу відеоконференції, дозволяє стиснути відеодані та водночас зберегти задані характеристики якості, а також канал, за яким ці дані можна буде

передати з прийнятною швидкістю. Як правило, в комплекс таких термінальних пристроїв для відеоконференції входить центральний пристрій – кодек з відеокамерою і мікрофоном, що забезпечує кодування/декодування аудіо- та відеоінформації, охоплення та відображення контенту; пристрій відображення інформації та відтворення звуку. У якості кодека на сучасному рівні розвитку техніки може використовуватися середньостатистичний персональний комп'ютер з програмним забезпеченням для відеоконференцій, що природно знижує вартість, витрати на установку обладнання, необхідного для застосування режиму відеоконференції [15].

Одним з актуальних аспектів застосування цифрових технологій у розслідуванні кримінальних правопорушень є проблема дослідження матеріалів, отриманих з використанням алгоритмів стиснення даних. Методи цифрового стиснення даних набули широкого поширення у системах запису мовної та графічної інформації. Усі формати запису, що використовуються у комп'ютерній техніці, засновані на певних алгоритмах стиснення.

Суттєвою перешкодою для використання в кримінальному процесі інформації, записаної із застосуванням алгоритмів стиснення, є те, що більшість з них засновано на видаленні з вихідного матеріалу так званої надлишкової інформації, яка за використання за звичайних умов не має ніякого значення. Однак для процесуального використання саме ця «непотрібна» інформація може бути принципово важливою, оскільки надає показанням або зображенню особливі неповторні ознаки, необхідні для встановлення автентичності. Адже першоджерелом інформації є людина або її мова. Така мова фіксується технічними пристроями, які надаються як доказ. Якщо мова передається каналами зв'язку, то перехоплюється і записується інформаційний процес, що протікає в каналах зв'язку. Зроблений запис переговорів вже є копією тих даних, які надсилалися через з'єднання.

Стиснення інформації, виконане з видаленням або корекцією певної її частини, необхідно розглядати як певний різновид монтажу, хоча воно і виконано автоматично, без втручання оператора. Такі матеріали вимагають обов'язкового експертного дослідження за використання їх у якості доказів у кримінальному судочинстві, оскільки за допомогою стиснення, виконаного з видаленням «зайвої» частини матеріалу, легше завуалювати зроблений раніше монтаж, а також позбавити запис індивідуальних ознак, унеможлививши встановлення його автентичності. Загалом інформаційні загрози можуть бути реалізовані 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 [16, с. 20].

Матеріали, отримані із застосуванням технічних засобів фіксації інформації під час застосування режиму відеоконференції, мають суттєві відмінності від інших матеріалів, що використовуються в ході розслідування кримінальних правопорушень. Оцінка таких доказів повинна проводитися з урахуванням критеріїв, відсутність або невідповідність яких заданим вимогам має бути правовою підставою для визнання досліджуваних доказів недопустимими.

До зазначених критеріїв слід віднести такі: процесуальна значущість, відповідність джерел отримання вимогам КПК України та можливість експертного підтвердження факту автентичності. Останній критерій повинен складатися з низки факторів, до яких можна віднести такі:

1) відсутність або допустимий для проведення експертних досліджень ступінь програмного стиснення даних;

2) відсутність в досліджуваних матеріалах ознак механічного або електронного монтажу;

3) відповідність записаної інформації місцю, часу, умовам та обставинам її отримання, зафіксованим у протоколі слідчої (розшукової) дії;

4) ідентифікація зразків та мови осіб, зафіксованих за допомогою технічних засобів, а також інші фактори [17].

Крім того, застосування технічних засобів у кримінальному провадженні повинно відповідати критеріям інформаційної безпеки, якими є такі:

1) доступність, яка означає, що інформація відкрита для доступу, а засоби її передавання функціонують, незважаючи на можливість вимкнення електроживлення, стихійні лиха, нещасні випадки або хакерські атаки;

2) аутентифікація, тобто підтвердження заявленої ідентичності користувачів;

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

4)конфіденційність – це захист повідомлень або збереженої інформації від несанкціонованого перехоплення й перегляду [18, с. 94].

До принципів забезпечення захисту інформації від несанкціонованого доступу, яких мають дотримуватися учасники кримінального провадження, А.А. Малюк, С.В. Пазизін, Н.С. Погожин відносять такі:

1) принцип обґрунтованості доступу, який полягає у виконанні таких умов, як достатня форма доступу для отримання інформації з необхідним для користувача рівнем конфіденційності та означена інформація, необхідна йому для виконання його процесуальних функцій;

2) принцип достатньої глибини контролю доступу, який визначає засоби захисту інформації, що містять механізми контролю доступу до всіх видів інформаційних та програмних ресурсів автоматизованих систем, які за принципом обґрунтованості доступу слід розподіляти між користувачами;

3) принцип 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;

4) принцип 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) принцип 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;

6) принцип цілісності засобів захисту, який передбачає, що засоби захисту інформації в автоматизованих системах повинні точно виконувати свої функції відповідно до вказаних вище принципів і бути ізольованими від користувачів, а також обладнаними спеціальним захищеним інтерфейсом для засобів контролю та сигналізації про спроби порушення захисту інформації та впливу на процеси в системі [16, с. 35–36].

Висновки. Отже, сучасні технології під час застосування режиму відеоконференції слід активно впроваджувати у кримінальне судочинство та використовувати їх на всіх стадіях розслідування та судового розгляду кримінальних проваджень. Впровадження у судочинство новітніх технічних розробок дозволить забезпечити не лише інформаційну безпеку під час використання технічних засобів і технологій у дистанційному кримінальному провадженні, а й допоможе вирішити комплекс проблем правового, організаційного та технічного характеру, дозволить підвищити ефективність правової системи.

Анотація

У статті досліджено проблеми забезпечення інформаційної безпеки під час використання технічних засобів і технологій у дистанційному кримінальному провадженні. Проаналізовано пріоритетні напрямки забезпечення надійності застосування систем відеоконференції. Визначено методи підвищення надійності систем застосування режиму відеоконференції та принципи забезпечення захисту інформації від несанкціонованого доступу. Доведено доцільність нормативно-правового закріплення загальної стратегії забезпечення інформаційної безпеки процесуальних дій, які проводяться в дистанційному кримінальному провадженні.

Ключові слова: кримінальне провадження, дистанційне провадження, режим відеоконференції, інформаційні технології, інформаційна безпека.

Аннотация

В статье исследованы проблемы обеспечения информационной безопасности при использовании технических средств и технологий в дистанционном уголовном производстве. Проанализированы приоритетные направления обеспечения надежности применения систем видеоконференции. Определены методы повышения надежности систем применения режима видеоконференции и принципы обеспечения защиты информации от несанкционированного доступа. Доказана целесообразность нормативно-правового закрепления общей стратегии обеспечения информационной безопасности процессуальных действий, проводимых в дистанционном уголовном производстве.

Ключевые слова: уголовное производство, дистанционное производство, режим видеоконференции, информационные технологии, информационная безопасность.

Bezanova A.V. Providing information security under the use of technical facilities and technologies in distance criminal proceedings

Summary

In the article the problems of providing information security during the use of technical means and technologies in remote criminal proceedings are investigated. The priority directions of ensuring the reliability of videoconferencing systems are analyzed. The methods of increasing the reliability of the systems of video conferencing mode and the principles of providing information security protection against unauthorized access are determined. The expediency of legal and legal consolidation of the general strategy of providing information security of procedural actions, which are carried out in remote criminal proceedings.

Key words: criminal proceedings, remote procedure, videoconferencing mode, Information Technology, informational security.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. / Офіційний вісник України. 2012. № 37. Ст. 1370.
2. Хабло О.Ю. Степанов О.С., Климчук М.П. Курс лекцій з кримінального процесу за новим Кримінальним процесуальним кодексом України (особлива частина). К., 2012. 284 с.
3. Моїсєєв О.М. Інформаційна безпека допиту експерта в режимі відеоконференції. Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки». Том 27 (66). 2014. № 4. С. 184–189.
4. Книженко С.О., Деменко Т.В. Особливості допиту в режимі відеоконференції під час досудового розслідування. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право». 2013. Випуск № 14. С. 208–214.

5. Синепол В., Цикин И. Системы компьютерной видеоконференцсвязи. М.: ООО «Мобильные телекоммуникации», 1999. 166 с.
6. Бортун М. Актуальні питання проведення допиту у режимі відеоконференції. Вісник Національної академії прокуратури України. 2014. № 1 (34). С. 64–70.
7. Лебедева К.Е., Лебедев Р.В., Мурыгин А.В. Методика повышения надежности видеоконференцсвязи. Сибирский журнал науки и технологий. 2017. Т. 18, № 2. С. 274–282. URL: http://cyberleninka.ru/article/n/metodika-povysheniya-nadezhnosti-videokonferentssvyazi (дата звернення: 29.03.2018).
8. Стрельцов А.А. и др. Организационно-правовое обеспечение информационной безопасности: учеб. пос. для студентов высш. учеб. завед. / под ред. А.А. Стрельцова. М.: Изд. центр «Академия», 2008. 256 с.
9. Сезонова І.К. Інформаційна безпека в сучасних умовах. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали IV Міжнародної науково-практичної конференції. Харків, 2015. С. 412–415.
10. Боровик П. Обеспечение информационной безопасности при использовании технологии видеоконференцсвязи в органах внутренних дел. Комплексная защита информации: материалы XVI научно-практической конференции (г. Гродно (Республика Беларусь), 17–20 мая 2011 года). Гродно, 2011. С. 179–182.
11. Белашенкова Н., Елизаров В., Семерханов И. Исследование проблем обеспечения информационной безопасности при проведении видеоконференций. Сибирский журнал науки и технологии. 2011. Том 18. № 2. СПб: Изд-во Ун-та ИТМО. С. 274–282.
12. Прохоров В., Манакова И. Построение интернет-видеосистем в условиях существенно ограниченной пропускной способности каналов связи Аграрный вестник Урала. 2015. № 3 (133). С. 34–38.
13. Павлов А., Датьев И. Протоколы маршрутизации в беспроводных сетях. Труды Кольского научного центра РАН. Апатиты: КнЦ РАН, 2014. С. 64–75.
14. Коханович Г., Вербицкий И. Метод динамического перераспределения потоков между портами устройства пакетной коммутации, позволяющий увеличить нагрузку сетевого оборудования. Математические машины и системы. Киев: Ин-т проблем математических машин и систем Национальной академии наук Украины, 2005. С. 148–160.
15. Скворцов Р.И. Проведение допроса с использованием средств видеоконференцсвязи: современное состояние и перспективы развития. Вестник Краснодарского университета МВД России. 2010. URL: http://cyberleninka.ru/article/n/provedenie-doprosa-s-ispolzovaniem-sredstv-videokonferentssvyazi-sovremennoe-sostoyanie-i-perspektivy-razvitiya (дата звернення: 29.03.2018).
16. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-Телеком, 2001. 148 с.
17. Бормотова Л.В. Особенности информационно-коммуникационного обеспечения уголовного судопроизводства. Вестник Оренбургского государственного университета. 2013. С. 24–27.
18. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза: монография. М.: ЮНИТИ-ДАНА, 2011. 196 с. URL: http://spkurdyumov.narod.ru/smirnov.pdf (дата звернення: 29.03.2018).