

Нагнибіда В. І.,доктор юридичних наук, професор,
завідувач наукової лабораторіїНауково-дослідного інституту приватного права і підприємництва
імені академіка Ф. Г. Бурчака

Національної академії правових наук України

ВЕРИФІКАЦІЯ СТОРІН ТА БЕЗПЕКА КАНАЛІВ ЗВ'ЯЗКУ ПРИ ВИРІШЕННІ СПОРІВ В АРБІТРАЖІ В РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ

Анотація. У статті досліджуються умови, принципи та підходи, за виконання або дотримання яких може гарантуватися належна верифікація сторін та забезпечуватися конфіденційність (включно із закритістю та доступністю лише для авторизованих користувачів) каналів зв'язку при вирішенні спорів у порядку арбітражу в режимі відеоконференції. Стверджується, що саме організація віртуальних слухань за допомогою відеоконференц-зв'язку, поруч із системами електронного обміну документами у справі, посідає чільне місце серед сучасних елементів онлайн-арбітражу. У світлі цього та зважаючи на конфіденційний характер арбітражного розгляду очевидною турботою для сторін та, відповідно, завданням складу арбітражу, що повинен забезпечити належний процес, який відповідатиме всім засадам, встановленим *lex arbitri*, є гарантування безпеки відеоконференц-зв'язку через шифрування або інші методи авторизованого доступу, включно з попередньою верифікацією сторін.

Автор резюмує, що більшість арбітражних регламентів не передбачають конкретних вимог до організації відеоконференц-зв'язку, здійснюючи лише загальні відсилання до цього засобу комунікації, фактично залишаючи ці питання для їх окреслення на рівні рекомендацій, керівництв, найкращих практик, звітів з приводу використання сучасних технологій у арбітражному розгляді та подібних їм документів. Відзначається, що на рівні таких джерел рекомендаційного характеру обов'язковість ідентифікації учасників відеоконференції та гарантування її конфіденційності і безпеки виокремлюються як базові принципи та вимоги до проведення слухань у форматі відеоконференції. При цьому допоки питання верифікації учасників відеоконференції значною мірою засновуються на попередній комунікації між сторонами та складом арбітражу, ключовим при гарантуванні безпеки каналів зв'язку є вибір та правильне застосування спеціального програмного забезпечення для відеоконференц-зв'язку, як такого, що пропонується третіми особами, так і розробленого в рамках цілісних систем онлайн-арбітражу, імplementованих у роботу відповідних арбітражних центрів та інститутів. Важливість таких застосунків підтверджується тим фактом, що до найважливіших характеристик платформ для організації відеоконференц-зв'язку (віртуальних слухань) сторони арбітражного розгляду традиційно, поруч із легкістю доступу, дружнім до користувача інтерфейсом, можливістю ефективного контролю з боку адміністратора, визначали й надійні функції безпеки, включаючи захист доступу за паролем, повідомлення для всіх учасників,

коли одним із учасників здійснюється запис засідання, а також наскрізне шифрування.

Ключові слова: міжнародний комерційний арбітраж, відео-конференція, учасники арбітражного розгляду, онлайн-арбітраж, процедура верифікації.

Постановка проблеми. На сьогодні арбітражна наука та практика, у розвиток дослідження загальних принципів запровадження процедур онлайн-арбітражу, про ефективність та повсюдність використання яких вже цілком можемо говорити, все частіше звертається до прикладних аспектів реалізації відповідних засобів і механізмів. Ключове місце серед останніх посідає відеоконференція або система відеоконференц-зв'язку як сучасна технологія телекомунікації за допомогою мережі Інтернет в режимі реального часу, яка забезпечує широкі можливості для сторін та складу арбітражу не лише в проведенні усних слухань і засідань, але й миттєвому обміні інформацією – файлами (заявами, доказами, арбітражними ухвалами тощо [1]). Зважаючи на конфіденційний характер арбітражного розгляду очевидною турботою для сторін та, відповідно, завданням складу арбітражу, що повинен забезпечити належний процес, який відповідатиме всім засадам, встановленим *lex arbitri*, є гарантування безпеки відеоконференц-зв'язку через шифрування або інші методи авторизованого доступу, включно з попередньою верифікацією сторін.

На перший погляд проблематика постає суто технологічною за своєю природою, проте використання відеоконференц-зв'язку в арбітражі прямо стосується не лише процесуальних аспектів, але й, як наслідок дотримання чи недотримання належної процедури, можливості визнання та виконання ухваленого арбітражного рішення. Адже невідповідність арбітражного процесу угоді сторін або *lex arbitri*, як і те, що сторона, проти якої винесено рішення, не була належним чином повідомлена про призначення арбітра чи про арбітражний розгляд або з інших причин не могла подати свої пояснення (в тому числі в режимі відеоконференції) є підставами для відмови у визнанні та приведенні до виконання арбітражного рішення (ст. V(1)(b)(d) Конвенції ООН про визнання та приведення до виконання іноземних арбітражних рішень, загальновідомої як Нью-Йоркська конвенція [2]). Відповідно озвучені вище питання є актуальними й з точки зору процесуальних аспектів організації та проведення арбітражного розгляду.

Аналіз останніх досліджень і публікацій. Питанням сутності та значення, формам впровадження та пов'язаним

проблемам використання технологій відеоконференц-зв'язку у міжнародному комерційному арбітражі, а також загальним концептам онлайн-арбітражу та віртуального арбітражного процесу, присвячували свої праці такі українські та зарубіжні вчені як Б. Х. Аламдарі, І. Амро, С. Ашауер, Д. Бешоу, Г. Борн, С. Вільске, Р. Волфф, Т. Десковскі, П. Джонсон, Б. О. Джуппоні, М. Замроні, Дж. Кауфманн-Колер, С. О. Кравцов, М. Ф. Лабаньє, К. Ларкін, Дж. Метьюз, Т. Моханта, Х. Дж. Наон, А. Пател, М. Пірс, В. Ю. Полатай, Ю. Д. Придика, К. Ренехан, К. М. Руні, К. Севарт, Л. Фроммельт, С. Халла, М. Шерер, Дж. Шерман та інші. При цьому конкретиці процесуального забезпечення та гарантування ефективності використання в онлайн-арбітражі засобів відеоконференц-зв'язку та вирішенні пов'язаних із цим практичних труднощів досі присвячено недостатньо наукових праць.

Таким чином, **метою статті** є, на основі звернення до арбітражних регламентів провідних арбітражних інституцій світу, документів рекомендаційного характеру та відповідної арбітражної практики, встановлення умов, принципів та підходів, за яких гарантується належна верифікація сторін та забезпечується конфіденційність (закритість, доступність лише для авторизованих користувачів) каналів зв'язку при вирішенні спорів у порядку арбітражу в режимі відеоконференції.

Виклад основного матеріалу дослідження. Як ми встановили у наших попередніх дослідженнях з проблематики, можливість звернення сторін та складу арбітражу до проведення слухань у режимі відеоконференції закріплюється, а відповідні механізми імплементуються у арбітражний процес більшістю арбітражних регламентів визнаних світових постійно діючих установ [3, с. 38–39]. До прикладу, відеоконференція як спосіб проведення конференцій з ведення справи передбачається ст. 24(4) Арбітражного регламенту Міжнародного арбітражного суду Міжнародної торговельної палати (*International Court of Arbitration – ICC*) у редакції від 1 січня 2021 року [4], ст. 14.3, ст. 19.2 Арбітражного регламенту Лондонського міжнародного арбітражного суду (*London Court of International Arbitration – LCIA*) у редакції від 1 жовтня 2020 року [5], ч. 2 ст. 47 Регламенту Міжнародного комерційного арбітражного суду при Торгово-промисловій палаті України (далі – МКАС при ТПП України) в редакції від 1 січня 2023 року [6] та ін.

При цьому необхідно вказати на те, що більшість арбітражних регламентів не передбачають конкретних вимог до організації відеоконференц-зв'язку, здійснюючи лише загальні відсилання до цього засобу комунікації, фактично залишаючи ці питання для їх окреслення на рівні рекомендацій, керівництв, найкращих практик, звітів з приводу використання сучасних технологій у арбітражному розгляді та подібних їм документів. Виключенням з цього правила може вважатись Регламент МКАС при ТПП України, який у ч. 3 ст. 47 необхідність зазначити у заяві МКАС від сторони про участь в усному слуханні у режимі відеоконференції ім'я та прізвище осіб, які будуть брати участь у засіданні Арбітражного суду в режимі відеоконференції, а також контактні дані, у тому числі електронну пошту, на яку секретаріат МКАС направить технічну інформацію, необхідну для підключення до відеоконференції, а також додати до заяви документи, що підтверджують повноваження цих осіб та їхню ідентифікацію.

Крім цього, визначається, що спосіб ідентифікації представника сторони, за допомогою якою він братиме участь

у відеоконференції із використанням власних технічних засобів, повинен бути прийнятним для складу арбітражу, а ризики технічної неможливості участі у відеоконференції поза межами приміщення МКАС, переривання зв'язку тощо несе сторона справи, яка подала відповідну заяву. Додатково згадка про верифіковані адреси електронної пошти сторін, на які здійснюється розсилка процесуальних документів у справі здійснюється у п. 10 Рекомендацій МКАС при ТПП України (ICAC) щодо подання документів у електронній формі [7].

Разом з тим, зрозуміло, що наведені положення вказаних регламентів є нормами загального характеру, та не торкаються безпосередньо порядку верифікації та/або гарантування безпеки (невтручання сторонніх осіб під час відеоконференц-зв'язку та конфіденційності переданої за його допомогою інформації загалом) і надійності з'єднання при проведенні відеоконференцій. Як відзначається у Звіті ICC з арбітражу та комісії APC щодо використання технологій для чесного, ефективного та дієвого міжнародного арбітражного розгляду 2022 року, організація слухань за допомогою відеоконференції викликає проблеми, відмінні від звичайних, фізичних засідань, з приводу чого арбітражною спільнотою на різних рівнях запропоновані вказівки або рекомендації із впровадження найкращих практик [1].

Під егідою того ж ICC, попередньо в рамках розробки заходів для протидії впливу пандемії COVID-19 на арбітражний процес, а сьогодні – уже в межах загальних рекомендацій щодо організації арбітражного розгляду відповідно до Регламенту ICC, підготовлено контрольний Чек-лист для протоколу про віртуальні слухання (далі – Чек-лист ICC) [8]. Документ визначає перелік питань, що потребують вирішення або погодження складом арбітражу і сторонами, та розбитий на кілька тематичних секцій, пов'язаних із організацією відеоконференцій (віртуальних слухань) та з дотриманням процесуальних принципів арбітражного розгляду під час їх проведення.

Так, до підготовчого плану, зокрема, віднесено пункти щодо: 1) узгодження кількості та списку учасників (арбітрів, сторін, адвокатів, свідків, експертів, адміністративних секретарів, перекладачів, стенографістів, техніків тощо); 2) визначення всіх місць лог-іну та точок підключення; 3) погодження, що кожна особа, присутня у кожній віртуальній кімнаті, буде ідентифікована на початку відеоконференції. Чек-лист ICC також перелічує необхідність проведення консультацій між складом арбітражу та сторонами щодо: 1) запису віртуального слухання (аудіовізуальний запис, конфіденційність запису та цінність запису порівняно з будь-яким створеним письмовим протоколом тощо); 2) будь-яких основних вимог або стандартів конфіденційності, які можуть вплинути на доступ або підключення певних учасників; 3) мінімальні вимоги до шифрування для захисту цілісності та безпеки віртуального слухання від будь-якого злому, незаконного доступу тощо.

Отже, на основі вищевикладеного, можемо виокремити обов'язковість ідентифікації учасників відеоконференції та гарантування її конфіденційності і безпеки серед базових принципів та вимог до проведення слухань у відповідному форматі, що буде справедливим для арбітражного розгляду відповідно до будь-якого регламенту провідної арбітражної інституції. Більш розгорнуті вказівки з приводу конкретних способів та шляхів втілення цих принципів на практиці можливо прослідкувати у інших документах ICC. Зокрема, звернення до Записки для

сторін та складу арбітражу стосовно проведення арбітражу відповідно до Арбітражного регламенту ICC від 1 січня 2021 року (далі – Записка ICC) [9], дозволяє ствердити, що проблема безпеки каналів зв'язку прямо пов'язана із використанням сторонами та складом арбітражу програмним забезпеченням під час відеоконференц-зв'язку – платформами для організації віртуальних слухань.

Серед найважливіших характеристик останніх сторони арбітражного розгляду традиційно, поруч із легкістю доступу, дружнім до користувача інтерфейсом, можливістю ефективного контролю з боку адміністратора, визначали й надійні функції безпеки, включаючи захист доступу за паролем, повідомлення для всіх учасників, коли одним із учасників здійснюється запис засідання, а також наскрізне шифрування. Відповідність програмного забезпечення для проведення віртуальних слухань цим вимогам є безумовною запорукою гарантування конфіденційності арбітражного процесу загалом.

На сьогодні відповідні платформи та застосунки є широко представленими на ринку. ICC у аналізованій Записці пропонує перелік доступних (рекомендованих) для сторін арбітражного розгляду за Арбітражним регламентом ICC платформ, вказуючи на те, що вони варіюються залежно від спеціально розроблених застосунків для індивідуальних потреб до загальнодоступних та навіть безкоштовних платформ. При цьому відзначається, що спеціалізовані або ліцензовані платні платформи для проведення відеоконференцій можуть забезпечувати більший рівень безпеки, конфіденційності та захисту даних, ніж публічні платформи безкоштовного використання. У будь-якому випадку закономірною є необхідність проведення попередніх консультацій між складом арбітражу та сторонами щодо вибору та апробації конкретного програмного забезпечення, його відповідності специфіці конкретного спору та побажанням сторін, у тому числі стосовно використання лише ліцензійних програм, налаштованих на максимально можливий рівень безпеки (шифрування).

У Записці ICC у зв'язку з цим окремо перелічується, що ICC має ліцензований доступ до таких варіантів платформи для відеоконференцій як *Microsoft Teams*, *VidyoCloud* і *Skype* для бізнесу (інші платформи, які нещодавно використовувалися у практиці ICC, включають *Zoom*, *Blue Jeans* і *GoToMeeting*). При цьому технічна підтримка ICC доступна дистанційно, щоб допомогти арбітражним судам використовувати такі платформи, приєднатися до наради (або слухання), керувати функціями аудіо та відео під час зустрічі та керувати функціями спільного використання екрана.

У літературі та професійних веб-джерелах називають й інші платформи, багато з яких не лише надають можливість проведення відеоконференцій (віртуальних слухань), але є комплексними системами управління справами (донедавна *NetCase* у ICC, що зараз працюю над новим, унікальним рішенням, *WIPO eADR* Всесвітньої організації інтелектуальної власності, *CIETAC Online Hearing System* Міжнародної економічної та торговельної комісії, численні онлайн-платформи Американської Арбітражної Асоціації – *CaseShield by AAA-ICDR*, *AAA WebFile*, *Panelist eCenter* тощо [10, с. 469–472]), а також додаткові опції в аспекті вибору спеціального програмного забезпечення для організації безпечного відеоконференц-зв'язку, обміну файлами, передачі зображення екрану та ін. (*Endispute*, *Legaler*, *Transperfect*, *Trustpoint.one* тощо [11]).

Спеціальне положення щодо попередньої ідентифікації усіх учасників відеоконференції містить Сеульський протокол про відеоконференції у міжнародному арбітражі, що покликаний слугувати посібником із найкращої практики з питань планування, тестування та проведення відеоконференцій у міжнародному арбітражі [12]. П. 3.1 Протоколу встановлює, що під час відеоконференції єдиними особами, присутніми у Віддаленому місці (*Remote Venue*), є Свідок, який дає свідчення (з його/її адвокатом, якщо вони є), перекладачі, помічники юристів для допомоги з документами та представники юридичної команди кожної зі Сторін. Кожна Сторона повинна надати іншій Стороні/Сторонам і Складу арбітражу ідентифікаційні дані кожної особи в кімнаті до початку відеоконференції, а Склад арбітражу повинен вжити заходів для перевірки особи (ідентифікації) кожної особи, присутньої на початку відеоконференції. Додаток 1 до Сеульського протоколу окремо торкається й технічних специфікацій для обладнання (та програмного забезпечення), що засновуються на загальних галузевих стандартах, рекомендованих Міжнародним союзом телекомунікацій – спеціалізованою агенцією Організації Об'єднаних Націй у галузі телекомунікацій, які призначені для того, щоб служити вказівкою щодо технічних специфікацій, які має забезпечити кожне місце проведення відеоконференцій.

Окремо варто звернутись й до положень, сформульованих у спільному Протоколі щодо кібербезпеки у міжнародному арбітражі 2022 року, підготовленому Міжнародною Радою з комерційного арбітражу (*International Council for Commercial Arbitration – ICCA*), Колегією адвокатів Нью-Йорку (*NYC Bar*) та Міжнародним інститутом із запобігання та вирішення конфліктів (*International Institute for Conflict Prevention and Resolution – CPR*) (далі – Протокол щодо кібербезпеки), за підтримки Постійної палати третейського суду (*Permanent Court of Arbitration – PCA*) [13]. Центральним аспектом Протоколу щодо кібербезпеки, власне, є визначення розумних та достатніх заходів безпеки щодо інформації для окремих арбітражних справ, надання процедурних та практичних вказівок для оцінки ризиків безпеки та визначення доступних заходів, які можна вжити у цьому напрямку.

У контексті верифікації учасника відеоконференції та безпеки каналів зв'язку можливим є звернення до рекомендацій Протоколу щодо кібербезпеки в частині заходів захисту інформації під час слухань і конференцій. Такі заходи можуть включати процедури обробки будь-яких стенограм, записів або відеозаписів; обмеження на те, яку техніку (наприклад, ноутбуки, планшети та смартфони) учасники можуть приносити та використовувати на слуханнях (особистих чи повністю або частково дистанційних); особливості та налаштування будь-яких платформ відеоконференц-зв'язку, які можуть використовуватися під час арбітражу; а також створення протоколу, включаючи відповідні заходи безпеки, для дистанційної дачі свідчень і проведення слухань.

Крім цього питання контролю доступу та фізичної безпеки визначаються документом як категорії, що, серед іншого, є важливими у цьому світі. Для контролю доступу Протокол щодо кібербезпеки звертає увагу на важливість моніторингу стану доступу до інформації, пов'язаної із арбітражним розглядом, включно з доступом до будь-яких систем, служб, пристроїв або додатків, які містять таку інформацію, до яких доступ повинен бути обмежений лише уповноваже-

ними особами, зокрема за принципом необхідного знання (*need-to-know*). Вони також можуть розглянути політику, яка застосовуватиметься в арбітражі щодо контролю облікових записів користувачів, паролів і багатфакторної автентифікації (зокрема, якщо спільна платформа використовується для розміщення даних, пов'язаних з арбітражем), або щодо протоколів віддаленого доступу.

Висновки. Таким чином, допоки питання верифікації учасників відеоконференції значною мірою засновуються на попередній комунікації між сторонами та складом арбітражу (включно з отриманням веб-посилання, паролю чи наданням учасникові попереднього доступу іншим чином до відеоконференції) ключовим при гарантуванні безпеки каналів зв'язку є вибір та правильне застосування спеціального програмного забезпечення для відеоконференції зв'язку, як такого, що пропонується третіми особами, так і розробленого в рамках цілісних систем онлайн-арбітражу, імплементованих у роботу відповідних арбітражних центрів та інститутів. Сучасний стан розвитку останнього вказує на фактично повсюдне втілення інструментів онлайн-арбітражу, включно з організацією та проведенням віртуальних слухань, у практиці розгляду арбітражних спорів.

Література:

1. ICC Arbitration and ADR Commission Report on Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings 2022. ICC Commission on Arbitration and ADR. URL: <https://iccwbo.org/wp-content/uploads/sites/3/2022/02/icc-arbitration-and-adr-commission-report-on-leveraging-technology-for-fair-effective-and-efficient-international-arbitration-proceedings.pdf>.
2. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958). *United Nations Organization*. URL: <https://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/New-York-Convention-E.pdf>.
3. Нагнибіда В. І. Процесуальні гарантії учасників арбітражного розгляду при вирішенні міжнародних комерційних спорів в режимі відеоконференції зв'язку. *Юридична Україна*. 2023. № 4. С. 38–46.
4. 2021 Arbitration Rules. International Court of Arbitration. URL: <https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/rules-procedure/2021-arbitration-rules/>.
5. 2020 LCIA Arbitration Rules. URL: https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx#Article%2014.
6. Регламент Міжнародного комерційного арбітражного суду при Торгово-промисловій палаті України. Зі змінами, що набрали чинності з 01.01.2023 р. URL: https://icac.org.ua/wp-content/uploads/Reglament-UA_2023.pdf.
7. МКАС при ТПП України (ICAC) щодо подання документів у електронній формі. URL: https://icac.org.ua/wp-content/uploads/Rekomendatsiyi-ISAS_elektronni-dokumenty_ukr.pdf.
8. Checklist for a Protocol on Virtual Hearings and Suggested Clauses for Cyber-Protocols and Procedural Orders Dealing with the Organisation of Virtual Hearings. URL: <https://iccwbo.org/wp-content/uploads/sites/3/2020/12/icc-checklist-cyber-protocol-and-clauses-orders-virtual-hearings-english.pdf>.
9. Note to Parties and Arbitration Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration. 1 January 2021. URL: <https://iccwbo.org/wp-content/uploads/sites/3/2020/12/icc-note-to-parties-and-arbitral-tribunals-on-the-conduct-of-arbitration-english-2021.pdf>.
10. Кравцов С. О. Онлайн платформи – запорука ефективного розгляду спорів в міжнародному комерційному арбітражі. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 462–476.
11. Technology Resources for Arbitration Practitioners – Virtual Arbitrations. International Bar Association. URL: <https://www.ibanet.org/technology-resources-for-arbitration-va>.
12. Seoul Protocol on Video Conferencing in International Arbitration. URL: <https://www.33bedfordrow.co.uk/upload/files/Seoul%20Protocol%20on%20Video%20Conference%20in%20International%20Arbitration.pdf>.
13. ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2022 Edition). URL: https://cdn.arbitration-icca.org/s3fs-public/document/media_document/ICCA-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration-2022-edition.pdf.

Nahnybida V. Verification of parties and security of communication channels when resolving disputes in arbitration in video conference mode

Summary. The article examines the conditions, principles and approaches, the implementation or observance of which can guarantee proper verification of the parties and ensure the confidentiality (including the closure and availability only to authorized users) of communication channels in the resolution of disputes in arbitration in videoconference mode. It is argued that it is the organization of virtual hearings by means of video conferencing, next to systems of electronic exchange of documents in the case, that occupies a prominent place among the modern elements of online arbitration. In light of this, and given the confidential nature of the arbitration proceedings, an obvious concern for the parties and, accordingly, the task of the arbitral tribunal, which must ensure due process that will meet all the principles established by the lex arbitri, is to ensure the security of the video conference through encryption or other methods of authorized access, including preliminary verification of the parties.

The author summarizes that most arbitration regulations do not provide for specific requirements for the organization of videoconferencing, making only general references to this means of communication, in fact leaving these issues to be outlined at the level of recommendations, guidelines, best practices, reports on the use of modern technologies in arbitration proceedings and similar documents. It is noted that at the level of such sources of a recommendation nature, the obligation to identify the participants of the video conference and guarantee its confidentiality and security are singled out as basic principles and requirements for conducting hearings in the format of a video conference. At the same time, while the verification of video conference participants is largely based on prior communication between the parties and the arbitral tribunal, the key to guaranteeing the security of communication channels is the selection and correct application of special software for video conference communication, such as that offered by third parties, as well as developed within the framework of integrated online arbitration systems, implemented in the work of the relevant arbitration centers and institutions. The importance of such applications is confirmed by the fact that among the most important characteristics of platforms for organizing video conferencing (virtual hearings) parties to arbitration proceedings, along with ease of access, a user-friendly interface, and the possibility of effective control by the administrator (host), also define reliable security functions, including password protection, notification to all participants when one participant is recording a meeting, and end-to-end encryption.

Key words: international commercial arbitration, video conference, participants to the arbitration, online arbitration, verification procedure.