ОСОБЛИВОСТІ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В СИСТЕМІ МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИН

І. В. ЛИТВИН, магістрант
Харківський національний університет міського господарства імені О. М. Бекетова, м. Харків

З розвитком цифрових технологій і популяризацією електронної комунікації в процесі арбітражного розгляду питання захисту персональних даних і забезпечення кібербезпеки набувають особливого значення. Про це свідчить дедалі більше кібератак, спрямованих на отримання несанкціонованого доступу до даних, що передаються в Міжнародному комерційному арбітражному. Зокрема, як показує статистика, тільки в 2018 році було зафіксовано більше 70 випадків несанкціонованого доступу до конфіденційних даних користувачів хмарних сховищ, в тому числі використовуваних при проведенні арбітражних розглядів, що призвело до втрати понад 1,3 млрд. записів.

Визнаючи цей факт, Міжнародна рада з комерційного арбітражу (International Council for Commercial Arbitration) спільно з Міжнародним інститутом по запобіганню і вирішенню конфліктів (International Institute for Conflict Prevention and Resolution) і Асоціацією адвокатів Нью-Йорка (New York Bar Association) створили Робочу групу з кібербезпеки в арбітражі (Working Group on Cybersecurity in Arbitration). Підсумком її роботи став представлений в листопаді 2019 Протокол з кібербезпеки в міжнародному арбітражі (Protocol on Cybersecurity in International Arbitration (2020 Edition).

З огляду на те, що забезпечення кібербезпеки є загальним обов'язком всіх учасників арбітражного розгляду, в Протоколі особливо наголошується, що безпеку відповідної інформації в кінцевому підсумку залежить від відповідальної поведінки та пильності учасників процесу, і, в першу чергу, сторін спору.

Важливою особливістю даного Протоколу є також той факт, що він не встановлює єдиних заходів, необхідних для забезпечення кібербезпеки, а лише створює основу для їх визначення з урахуванням всіх обставин конкретної справи. При цьому даний документ спрямований як на конфліктуючі Сторони, так і на склади арбітражу, які розглядають конкретний спір, і арбітражні інститути, що здійснюють адміністрування суперечок (Принцип 1 Протоколу).

Ще один важливий документ в даній області − Керівництво з кібербезпеки, розроблене в 2018 р в рамках Міжнародної асоціації юристів (МАЮ). Воно містить заходи, спрямовані на мінімізацію загрози кібербезпеки, і орієнтовані на компанії і індивідуальних підприємців.

Ще одним важливим напрямком роботи в галузі захисту персональних даних і забезпечення кібербезпеки в міжнародному комерційному арбітражі є створення комунікаційних платформ, які дозволяють сторонам і арбітрам обмінюватися процесуальними документами без необхідності їх пересилання за

допомогою електронних засобів зв'язку та інших погано захищених способів обміну документами.

Одним з перших таку платформу створив Арбітражний інститут Торгової палати Стокгольма (далі – Арбітраж ТПС). Зокрема, починаючи з вересня 2019 року всі розгляди, що проводяться даними арбітражним інститутом, повинні адмініструватися за допомогою даної платформи [3]. Як наслідок, під час вступу спору до Арбітражного суду при ТПС, поряд з його реєстрацією створюється індивідуальний сайт справи, доступ до якого мають тільки учасники арбітражного розгляду. При цьому сторони отримують миттєвий доступ до файлів справи відразу після їх завантаження в систему, а також можуть самостійно завантажувати, переглядати і завантажувати матеріали як через комп'ютер, так і з мобільних пристроїв.

Література:

1. Cybersecurity in International Arbitration ICCA-NYC Bar-CPR Working Group. URL: https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html (дата звернення: 31.01.2021).

2. ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020 Edition). New York Arbitration Week Special Printing. The ICCA Reports No. 6. URL: https://www.arbitrationicca.org/media/14/76788479244143/icca-nyc_barcpr_cybersecurity_protocol_for_international_arbitration_-_print_ver sion.pdf (дата звернення: 31.01.2021).

3. Cyber Security Guidelines by the IBA`s Presidential Task Force on Cyber Security. October 2018. URL: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (дата звернення: 31.01.2021).

4. SCC Platform – Simplifying Secure Communication from Request to Award. URL: https://sccinstitute.com/scc-platform/ (дата звернення: 31.01.2021).