

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

**ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ
УКРАЇНИ В УМОВАХ ВІЙНИ
ТА ГЛОБАЛЬНИХ ВИКЛИКІВ ХХІ СТОЛІТТЯ:
СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ
ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ**

МАТЕРІАЛИ
Міжнародної науково-практичної
конференції

19 травня 2023 року

У двох томах

Том 1



Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова**.

Відповідальний за випуск **М. Р. Аракелян**.
Матеріали видано в авторській редакції.

Європейські орієнтири розвитку України в умовах війни та
Є24 глобальних викликів XXI століття: синергія наукових, освітніх
та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-
практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редак-
цією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. –
Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

© Національний університет
«Одеська юридична академія», 2023

3. Charter of the United Nations and Statute of the International Court of Justice. URL: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>
4. Гогоша О. Гуманітарна складова миротворчих операцій ООН. *Вісник Львівського університету. Серія «Міжнародні відносини»*. 2013. Вип. 32. С. 104–108.
5. Assistance in cases of natural disaster and other disaster situations. URL: <https://digitallibrary.un.org/record/201561>
6. United Nations *General Assembly Resolution 46/182* Strengthening of the coordination of humanitarian emergency assistance of the United Nations. URL: <https://documents-dds-ny.un.org/doc>
7. IASC Transformative Agenda. URL: <https://interagencystandingcommittee>
8. Cluster Approach (IASC). URL: <https://emergency.unhcr.org/coordination>
9. Chapeau and Compendium. URL: <https://interagencystanding>
10. United Nations Development Programme. <https://www.undp.org/UNDP>
11. UNDP resilience building and recovery programme. URL: <https://www.undp.org>
12. Доступність правової допомоги в контексті воєнного стану. file:///C:/Users/User/Downloads/dostupnist-pravovoyi-dopomogi-n.pdf

Ключові слова: гуманітарна допомога, ООН, ПРООН, IASC, Програма з підвищення стійкості та відновлення України.

Key words: humanitarian aid, UN, UNDP, IASC, Program for increasing the stability and recovery of Ukraine.

ГАЛАТ ВЛАДИСЛАВ ІГОРОВИЧ

*Національний університет «Одеська юридична академія»,
аспірант кафедри міжнародного та європейського права*

ІСТОТНІ ПОРУШЕННЯ МІЖНАРОДНОГО ДОГОВОРУ КУПВЛІ-ПРОДАЖУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК

Сучасні технології кидають нові виклики міжнародному співтовариству, та потреба в кібербезпеці та захист від кібератак є важливою складовою міжнародної безпеки.

Так, як кібератаки стали досить важливим атрибутом, для послаблення життєздатності країни, оскільки майже всі процеси оцифровані, вагоме місце в життєдіяльності та обороноздатності країни займає кіберзахист. Кожна країна шукає способи захисту від кібератак, за допомогою розроблення програмного забезпечення, яке буде захищати всі важливі ресурси країни від проникнення та націлене на знешкодження потенційної небезпеки викрадення інформації та порушення роботи різних систем в країні. Але розробка програмного забезпечення потребує великих фінансових затрат, тому країни, які розвиваються намагаються перейняти досвід розвинених країн і купити в них, вищезгадане програмне забезпечення та удосконалити і пристосувати під особливості та можливості країни, яка купила програмне забезпечення, для захисту від кібератак.

На сьогоднішній день існує багато країн, які виробляють програмне забезпечення для кіберзахисту. Однією з провідних країн-виробників є США. У США розташовуються провідні компанії з кібербезпеки, такі як Symantec, McAfee та Palo Alto Networks, які забезпечують захист від кібератак для багатьох країн, організацій та компаній по всьому світу. Є також країни, які займають вагоме місце в розробленні програмного забезпечення для кіберзахисту. Наприклад, Ізраїльські компанії такі як Check Point, CyberArk та NSO Group, розробляють програмне забезпечення для захисту від кібератак [3].

Кожна країна здійснює обмін даними з партнерами, для безпеки здійснення подібного обміну необхідно в план захисту включити договір про порядок організації обміну електронними даними, в якому відображаються наступні питання:

- розмежування відповідальності суб'єктів, що беруть участь в процесах обміну електронними документами;
- визначення порядку підготовки, оформлення, передачі, прийому, перевірки автентичності та цілісності електронних матеріалів;
- порядок вирішення спорів у разі виникнення конфліктів [1, с. 44].

Для України, як для країни, що розвивається, важливим питанням залишається, які ж саме складності виникають під час купівлі країною програмного забезпечення у міжнародних розробників, так як рівень розробників в Україні хоч і високий, але фінансування та необхідність пришвидшити та удосконалити захист від кібератак в часи збройної агресії проти України та постійних атак на урядові та інші ресурси країни, призводить до необхідності все більше і більше розвивати питання захисту від даного виду атак, змушують владу задумуватись над купівлею такого програмного забезпечення для захисту від кібератак, а також важливе питання посідає, саме дії що можуть призвести до порушення істотних умов договору при купівлі даного програмного забезпечення у міжнародних партнерів та компаній які займаються розробкою вищесказаного заходу захисту. Оскільки програмне забезпечення для захисту від кібератак є досить специфічним об'єктом, і часто використовується для захисту від викрадення важливої для країни інформації, договори прописуються досить детально і нагромаджуються безліччю пунктів, які наголошують умови, невиконання яких може призвести до порушень цього договору, починаючи від можливості удосконалення країною яка купила програмне забезпечення, навчання спеціалістів з використання даного програмного забезпечення, закінчуючи секретними пунктами, які можуть включати стратегічні питання захисту інформації на об'єктах критичної інфраструктури та в військовій сфері.

Найпоширенішими порушеннями, істотних умов міжнародного договору купівлі-продажу програмного забезпечення в сфері захисту від кібератак є:

- недотримання правил, пов'язаних зі зберіганням, передачею та захистом конфіденційної інформації, що може міститись в програмах кіберзахисту. Такі правила можуть бути зазначені в різних документах, зокрема, угодах про нерозголошення між країнами та міжнародними

компаніями, договорах на закупівлю, договорах про перехід прав власності тощо;

- невиконання вимог договору, пов'язаних з безпекою програмного забезпечення, що використовується в обороні. Це може включати в себе відсутність відповідної сертифікації, недостатній захист від вразливостей та інших загроз, а також відсутність механізмів захисту від несанкціонованого доступу до програмного забезпечення;

- крім того, в зв'язку зі специфікою предмету купівлі можуть бути порушені правила, пов'язані із закупівлею програмного забезпечення з певних країн або компаній, які знаходяться під санкціями, що встановлені міжнародними організаціями, що ми можемо бачити зараз на власні очі, коли підсанкційні країни отримують технології, для розробки програм, які можуть порушувати функціонування обороноздатності країни, шляхом відвантаження вірусних програм до системи захисту інших країн.

Отже, при закупівлі програмного забезпечення в сфері кіберзахисту в міжнародних партнерів та міжнародних компаній, покупці повинні брати до увагу кожен дрібницю яка повинна забезпечити цілісність, повноту та правильність договору, та містити тільки ті умови, які під силу виконати як продавець, так і покупець. Оскільки неправильно сформований договір, який містить умови, які заздалегідь неможливо виконати, можуть спричинити великі проблеми в безпекових питаннях країни, нікчемність або недійсність договору за яким відбувається покупка програмного забезпечення та може призвести до репутаційної і грошової відповідальності за невиконання істотних умов договору. Необхідно прописати всі питання, які є важливими для забезпечення максимального функціонування та виконання договору, які встановлені міжнародними договорами та іншими правовими актами, щоб уникнути можливі порушення та забезпечити максимальний рівень захисту від кібератак.

Список використаних джерел:

1. Цензура М. О. (2020). Захист електронних навчально-методичних видань від несанкціонованого доступу. [Кібергігієна. Кібербезпека. Безпека держави. Матеріали наукових семінарів]. Київ, 2020. URL: <https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf>
2. The Department of Defense Cyber Strategy. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf
3. Top 20 Cybersecurity Companies To Know in 2023. URL: [https://www.esecurityplanet.com/products/top-cybersecurity-companies/\(January 20, 2023\)](https://www.esecurityplanet.com/products/top-cybersecurity-companies/(January 20, 2023)).

Ключові слова: кібератака, кіберзахист, міжнародний договір купівлі-продажу, програмне забезпечення.

Key words: cyber attack, cyber defense, international sales contract, software.

Дронов Владислав Юрійович Екологічна інформація як вид інформації у національному та міжнародному праві: право на доступ	347
Zhebrovska Krystyna, Riaboshapchenko Anastasiia Universal system of international protection of human rights: general principles	349
Канєнберг-Сандул Оксана Константинівна Проблеми та перспективи захисту прав людини в режимі військової окупації	353
Кінаш Наталія Богданівна Адаптація законодавства України до актів Європейського Союзу як напрям європейської безпеки	356
Мануйлова Катерина Вікторівна Особливості захисту прав людини в умовах збройних конфліктів та глобальних викликів сучасності	359
Пасечник Олена Владиславівна Трансформація медичного законодавства України в умовах воєнного стану	361
Печерова Ніна Григорівна Право власності, режими використання об'єкту, що внесений до списку Всесвітньої спадщини ЮНЕСКО	363
Федорова Тетяна Сергіївна Ідея верховенства права у міжнародно-правовому дискурсі	366
Харитонов Роман Феліксівич, Замостенчук Анастасія Олександрівна Проблематика четвертого та п'ятого покоління прав людини	370
Цибульська Ольга Юріївна Окремі питання колізійних норм щодо правових наслідків шлюбу в умовах воєнного положення в Україні	372
Большакова Ольга Віталіївна Обмеження прав людини в умовах воєнного стану: законодавче врегулювання, межі, закордонний досвід	374
Hrebeniuk Dmytro Ai regulation in EU: the European Parliament's stand	377
Біляєвський Дмитро Сергійович Визначення та проблематика терміна «гібридна війна»	380
Бурдюжа Олександр Миколайович Правові основи діяльності ООН щодо гуманітарної допомоги	383
Галат Владислав Ігорович Істотні порушення міжнародного договору купівлі-продажу програмного забезпечення для захисту від кібератак	386