Список використаних джерел:

1. Кодекс законів про працю України : Закон України від 10.12.1971 №322-VIII [Електрон. ресурс]. Електрон. текст. дані. Режим доступу: https://zakon.rada.gov.ua/laws/show/322-08#Text, вільний (дата звернення: 27.10.2023). – Назва з екрана.

2. Петришак А., Казак К. Трудовий договір з нефіксованим робочим часом від “А” до “Я” [Електрон. ресурс]. Електрон. текст. дані. Режим доступу: https://buh.ligazakon.net/aktualno/12838_trudoviy-dogovr-z-nefksovanim-robochim-chasom-vd-a-do-ya, вільний (дата звернення: 27.10.2023). – Назва з екрана.

3. Дудін В. 10 запитань про 0-годинні контракти в Україні. [Електрон. ресурс]. Електрон. текст. дані. Режим доступу: https://rev.org.ua/10-zapitan-pro-0-godinni-kontrakti-v-ukra%D1%97ni/, вільний (дата звернення: 27.10.2023). – Назва з екрана.

ІНФОРМАЦІЙНА БЕЗПЕКА НА МИТНИЦІ В УМОВАХ ВОЄННОГО СТАНУ

КОРКІШКО Вадим Андрійович,
здобувач вищої освіти
Харківський національний університет
міського господарства імені О. М. Бекетова

Триваюча агресія з боку російської федерації та інші кардинальні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення комплексу заходів, направлених на захист громадян та державного суверенітету, протидію небезпеці, що виникла. Це тягне за собою перебудову організації роботи, життєдіяльності населення, діяльності підприємств тощо. Важливо посилити безпеку у всіх секторах, від сільського господарства до державних структур та їх підрозділів. Україна сьогодні долає виклики війни завдяки підтримці іноземних держав. Вона охоплює фінансову, гуманітарну, технічну, військову та різні інші види допомоги, які переміщуються безпосередньо через державний кордон, що реалізовується завдяки транспортним та інформаційним каналам зв’язку. Митна інформація, стає однією із пріоритетних цілей агресора та інших зацікавлених осіб, доступ до якої може призвести до виникнення значних збитків, а також порушення безпеки держави, тому забезпечення інформаційної безпеки (далі кібербезпеки) на митниці є важливим. Відповідно до Міжнародної конвенції про спрощення і гармонізацію митних процедур, створений та діє єдиний інформаційний центр між митними службами країн, що доєдналися до неї [1]. Відповідно до статті 544 Митного кодексу України, митні органи здійснюють митний контроль та виконання митних формальностей щодо товарів, транспортних засобів комерційного призначення, що переміщуються через митний кордон України, у тому числі на підставі електронних документів

(електронне декларування), за допомогою технічних засобів контролю; організація та управління митним органом відбувається із застосуванням електронної інформації [2].

Акцентуючи увагу на перевагах впровадження інформаційних технологій у сучасний світ, не можна забувати про появу нових загроз національній та міжнародній безпеці. В умовах війни зростає кількість і потужність кібератак, вмотивованих інтересами конкретних держав, груп та окремих осіб. З початку повномасштабного вторгнення під контроль росії потрапили митні пункти пропуску та контролю, та інші державні установи, громадська інфраструктура. В умовах сьогодення ризик кібератак на митні пости та пункти пропуску, та відповідні митні органи збільшився. Метою України повинно стати створення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідно: створення національної системи кібербезпеки; зміцнення потенціалу суб'єктів сектору безпеки і оборони для забезпечення ефективного реагування на кіберзагрози військового характеру; забезпечення безпеки електронних інформаційних ресурсів держави, інформації, що підлягає захисту відповідно до законодавства, та інформаційної інфраструктури, що перебуває під юрисдикцією України (критична інформаційна інфраструктура) [3]. Забезпечення кібербезпеки України в кіберпросторі досягається шляхом комплексного застосування низки правових, організаційних та інформаційних заходів і має базуватися на таких принципах: забезпечення національних інтересів України; відповідність та адекватність заходів кіберзахисту реальним і потенційним ризикам; пріоритет превентивних заходів; невідворотність покарання за кіберзлочини; пріоритетний розвиток і підтримка вітчизняного науково-технічного та виробничого потенціалу; міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення єдиних підходів протидії кіберзагрозам; активізація зусиль із розслідування та запобігання кіберзлочинам; міжнародне співробітництво з метою запобігання використанню кіберпростору в протиправних і військових цілях; забезпечення демократичного цивільного контролю над державними військовими та правоохоронними органами, що діють у сфері кібербезпеки, встановленого відповідно до законодавства України [3]. Стратегія ґрунтується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України № 2824-4 від 7 вересня 2005 року [4].

Підсумовуючи, Україна зіткнулася зі складною безпековою ситуацією. У відповідь на ці виклики необхідно перейти до режиму виживання, який надає пріоритет безпеці, людському життю та державному суверенітету. Це вимагає комплексної реструктуризації в різних секторах, приділяючи особливу увагу зміцненню безпеки, як фізичної, так і інформаційної. Конфлікт, що триває, підкреслює важливість захисту інформації, особливо у сфері митниці, що може мати серйозні наслідки. Визнаючи мінливий характер загроз, у тому числі збільшення кількості спонсорованих кібератак, важливим для України є посилення національної системи кібербезпеки. Важливим є

підвищення спроможності секторів безпеки та оборони реагувати на кіберзагрози, а також рівня забезпечення електронних інформаційних ресурсів та критичної інфраструктури. Зрештою, стратегія повинна узгоджуватися з положеннями Конвенції про кіберзлочинність, що забезпечить ефективний захист в умовах дедалі складнішого та динамічного безпекового середовища.

Список використаних джерел:

1. Міжнародна конвенція про спрощення і гармонізацію митних процедур [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_643#Text
2. Митний кодекс України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/4495-17#Text
3. Про Стратегію кібербезпеки України: Указ Президента України №96/2016 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/962016-19836
4. Про кіберзлочинність: Конвенція ратифікована Законом України від 7 вересня 2005 року № 2824-IV [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text

ПРАВОВЕ РЕГУЛЮВАННЯ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

ПАКУЛІНА Алевтина Анатоліївна,
канд. екон. наук, доцент,
СЕРГІЄНКО Анастасія Андріївна,
здобувач вищої освіти
Харківський національний університет
міського господарства імені О.М. Бекетова

Після оголошення на території України воєнного стану та початку активної фази бойових дій більша частина бізнесу була фактично паралізована через різноманітні обставини. А без економічної активності неможливе повноцінне функціонування держави в умовах воєнного стану. Саме з цією метою держава почала активно запроваджувати комплексні зміни до законодавства та державних програм, спрямованих на підтримку української економіки. В таких умовах єдиним можливим способом підтримки бізнесу стали лібералізація та посилення державної підтримки.

З самого початку і до сьогодення, всі зусилля держави спрямовані на захист суверенітету, територіальної цілісності та недоторканності України. Та досягти цього можливо лише тоді, коли поєднується два основні фронти. Першим виступає воєнний фронт, а другим – економічний. Схожої позиції дотримується А. Кузьменко, який переконує, що запуск потужного економічного фронту в сьогоднішні непрості часи є надзвичайно важливим для суспільства, адже без економічної активності неможливе повноцінне