СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

# РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

**У двох частинах**

**Частина 2**

Суми
Сумський державний університет
2020

законодавство в нашій країні, щоб у населення все ж була довіра до вітчизнянної медецини, після чого відкорегувати цивільне законодавство а в останню чергу кримінальне, або зробити це комплексно, що звістно є набагато складнішим процессом. В будь якому випадку данні зміни не відбуваються швидко і скоріше за все це, можливо, як план дій до розвитку на найближчі років 10.

Отже, потрібно також враховувати, що абсолютна недопустимість евтаназії в нашій країні не позбавляє думок, що пов'язані з стражданнями невиліковно хворих людей. Та не варто закривати очі й забувати про існування соціальної евтаназії в нашій країні, яка має насправді досить високий рівень. Тому дослідження даної теми, на наш погляд, є важливою потребою для нашої країни.

**ЛІТЕРАТУРА:**

1. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 р. № 2801-XII / Верховна Рада України. URL: https:/zakon.rada.gov.ua/laws/show/2801-12.

2. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

3. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III // *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

## СУЧАСНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ГЛОБАЛЬНИХ ЗАГРОЗ

***Думчиков М. О.***
*к. ю. н., асистент кафедри КПДС ННІ права*
*Сумського державного університету*
***Бондаренко О. С.***
*к. ю. н., старший викладач кафедри КПДС ННІ права*
*Сумського державного університету*

В умовах глобальних загроз забезпечення безпеки в світі, вимагає координації і врегулювання багатьох політичних і економічних питань. Зокрема, це осередки цивільних, міжетнічних конфліктів і воєн, продовольчі загрози, негативні наслідки зміни клімату, забруднення навколишнього середовища, виснаження природнихресурсів і уповільнення їх повторного відновлення. Однак серед усіх компонентівзабезпечення безпеки з'явився новий і одночасно складний елемент безпеки – кібербезпека.

Щорічно зростає збиток великих організацій, компаній, окремих громадян і ділових людей від кібер атак і нападів зловмисників. Згідно з прогнозами компанії Gartner щорічні

витрати корпорацій і компаній світу по підвищенню безпеки системи інформаційних технологій складають 76-77 млрд. дол. США [1]. А в цілому зростання кіберизиків за 2019 рік коштувала світовій економіці 445 млрд. дол. З цієї суми 108 млрд. припали на частку США. Ризики, пов'язані з кібершпіонажем і злочинами в сфері Інтернет-діяльності, продовжують нести все більші загрози для бізнесу. Половина витрат по запобіганню кіберризиків несли на собі економіки США, Китаю, Німеччини і Японії, що становить понад 200 млрд. дол. США.

Найбільш помітними кіберзлочинами є викрадення даних і порушення недоторканності приватного життя. У найближчі роки набере чинності крадіжка інтелектуальної власності, кібер-вимагання та диверсії високих технологій. Крім того, багато державних організацій та суб'єктів ринкових відносин, комерсанти і ділові люди надають мале значення проблемам і організації заходів по підвищенню надійної системи кібербезпеки, і в багатьох випадках для цього навіть не роблять елементарні кроки, і не проводять необхідних робіт з тих чи інших елементів кібербезпеки, щодо підвищення ефективності та раціональності захисних механізмів кіберпростору, стійкості і надійності Інтернет мережі.

У цих умовах потрібно детально розглянути і виявити основні фактори і причини, що спонукають вчинення хакерських атак для розробки нових, більш ефективних і максимально практичних механізмів у боротьбі проти хакерів і зловмисників, шкідників середовища кіберпростору і інфраструктури. Тим більше в умовах глобалізації та швидкого розширення географії хакерських атак, злочинних діянь кіберзлочинців і зловмисників необхідна координація і мобілізація розумових, інтелектуальних, наукових, людських ресурсів проти боротьби з кіберзлочинами в усьому світі. Всі ці елементи, механізми і компоненти повинні бути працездатними і адекватними щоденних проблем, що породжується в кіберпросторі.

Потрібні дієві, практичні заходи в багатьох областях інформаційного середовища системи кібербезпеки, і підвищення його стійкості. Фахівці Австрійського центру з кібербезпеки відзначають, що необхідно враховувати всі проблеми і питання напруженості у відносинах між недоторканністю в особистому житті і державної безпеки, захисту людей, в тому числі самої держави від кібератак, загроз кібервійни та кібертероризму, уважному спостереженню за кібершпіонажем з метою його припинення, забезпечення дієвих практичних запобіжних заходів його в кіберпросторі, дотримання етики, норм і міжнародного права [2].

Проблеми кібербезпеки є проблемами в світовому масштабу і одночасно новим напрямком для дослідників, тому невивчені елементи сфери кібербезпеки потребують

більш детальному розгляду, для вдосконалення протидії діяльності хакерів і зловмисників. Так, А.Кохен прийшов до висновку, що необхідно перенести центр уваги на злочини хакерів і кібератак, які найбільше пов'язані з масивними інформаційними або електронними ресурсами компаній і урядів країн світу. Прийшов час загострити нашу увагу на пріоритетних завданнях і забезпечити безпеку інформаційних масивів, і в цілому розробити нові стратегії для безпеки кіберпростору [3].

Дійсно, багато хто вважає, що нові і більш складні міжнародні загрози в особі кіберхакерів і зловмисників потребують побудови сильної та системної конструкції із захисту кіберпростору, щоб забезпечити повноцінну і ефективну кібербезпеку в світі. Потрібно максимальне підвищення безпеки своєї цифрової інфраструктури, розвиток наступальної, але, як було зазначено, ці заходи не гарантують повністю виключення кібератак і настання зловмисників, тобто проблеми кібербезпеки не гарантовані.

Кіберпростір гостро потребує зменшення наслідків системних загроз, які є наслідком властивої непередбачуваності комп'ютерів і інформаційної системи, які самі по собі створюють ненавмисні, іншими словами, потенційно або насправді небезпечні ситуації длялюдського середовища, в якому вони вмонтовані. Тобто, кіберзагроза виходить від програмного забезпечення, і не може бути виправлена за допомогою цифрової технології, вдосконалення його основ і програмування. Тому справедливо вказують на необхідність розробки і здійснення більш удосконалюваної концепції комп'ютерної безпеки в сфері кіберпростору, усвідомлення актуальності в широкому сенсі проблеми кібербезпеки і розвитку стратегій безпеки кіберпростору.

Проблема глибокого вивчення характеру і суті елементів і концептуальних основ кібербезпеки, його ефективності обумовлює необхідність вироблення єдиного, комплексного підходу до формування дієвих систем і механізмів кібербезпеки, розробки і здійснення раціональних заходів щодо функціонування кіберпростору, забезпечення його захисту від можливих кіберзлочинів, надійних механізмів і сервісів для протидія кібератакам, забезпечення застосування інтелектуальних методів щодо вдосконалення системи кібербезпеки, запобігання потрапляння вірусних частинок, своєчасного виявлення і нейтралізації атак і проникнень.

Відзначимо, що узагальнення і розкриття породжують причин і коріння кіберзлочинів, дії хакерів і зловмисників залишається однією з складних завдань у сфері забезпечення кібербезпеки в світі. Необхідно точно і широко скласти класифікацію та елементи небезпеки в кіберпросторі, вивчити їх характеристику і сутність з виділенням основних особливостей тактики і дії хакерів і зловмисників, і розробити адекватні механізми щодо припинення подібних злочинних діянь в кіберпросторі. Таким чином,

результати дослідження обумовлюють важливість усвідомлення і осмислення серйозних проблем, а питання забезпечення кібербезпеки світу вимагає розробки і здійснення більш ефективних механізмів функціонування і забезпечення роботи кіберпростору, підвищення надійності основних механізмів і компонентів глобальної Інтернет-мережі та інших пристроїв, комплексного і системного підходу в визначенні методичних засад і інструментаріїв формування державної політики з кібербезпеки в нинішніх умовах.

**ЛІТЕРАТУРА:**

1. Кибербезопасность: на что глобальне компании потратят $76,9 млрд. IT GROUP DF, 2014. URL: http://www. delo.ua.

2. Word Politics, Security and International Law in Cyber Space. Australian Centre for Cyber Security. UNSW, Canberra. URL: http://www.unsw.adfa.edu.au.

3. Cohen A. The Willie Sutton Theory of Cyber Security, 2015. URL: http://www.securityweek.com.

## КОРУПЦІЯ В ОБОРОННО-ПРОМИСЛОВОМУ КОМПЛЕКСІ УКРАЇНИ: СУЧАСНИЙ СТАН

***Пилипенко Є. С.***
*Студент ІІІ курсу ННІ права*
*Сумського державного університету*
***Науковий керівник: Думчиков М. О.***
*к. ю. н., асистент кафедри КПДС ННІ права*
*Сумського державного університету*

Нас змалку привчали до того, що добро завжди перемагає зло. В щасливому кінці кожної казки, яку з захватом розповідали нам увечері батьки, ми брали приклад з хороброго рицаря, який вміло проходив усі перепони, та залишав жахливих чудовиськ навіки у темниці. Але, на жаль, наше життя зовсім не схоже на казку.

Ми живемо у країні, яка знаходиться, мабуть, на найважчому на найважливішому етапі існування за всі роки своєї незалежності. Україну паралізують численні проблеми, основною з яких є корупція. Вона проникла в усі сфери життєдіяльності країни, повністю охопила галузі і регіони, завдаючи колосальної економічної шкоди, підриваючи основи держави і суспільної моралі. Як відомо, наявність корупції підриває довіру до влади і основним принципам державного управління, перешкоджає чесній конкуренції, ускладнює державний розвиток, загрожує національній безпеці, демократичним інститутам і моральним засадам суспільства.