

**ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ**



**КІБЕРБЕЗПЕКА В УКРАЇНІ:
ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ
ПИТАННЯ**

**International scientific-practical conference
"Cybersecurity in Ukraine: Legal and
Organizational Issues"**

**Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року**

**ОДУВС
м. Одеса
2022**

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**



**КІБЕРБЕЗПЕКА В УКРАЇНІ:
ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ**

**International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organizational Issues"**

**Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року**

Одеса
ОДУВС
2022

*Рекомендовано до друку рішенням кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного університету внутрішніх справ*

*Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції*

Кібербезпека в Україні: правові та організаційні питання:
К38 матеріали міжн. наук. практ. конф., м. Одеса, 23 листопада 2022 р.
Одеса : ОДУВС, 2022. 152 с.
ISBN 678-717-70204

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 23 листопада 2022 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), здобувачам вищої освіти першого та другого рівня освіти.

© ОДУВС, 2022

ОКРЕМІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Людмила РОТАРЬ

курсантка 302навчального взводу 3 курсу ФПФПКП

Ганна ФОРОС

*т.в.о. завідувача кафедри кібербезпеки
та інформаційного забезпечення ОДУВС,
к.ю.н., доцент*

Сьогодні використання віртуальних середовищ досягло свого піку. Громадяни або юридичні особи незалежно від їх організаційно-правової форми користуються. Він задовольняє будь-які потреби – особисті чи ділові. За рахунок використання кіберпростору може бути багато питань, які потрібно вирішити. Варто підкреслити, що адміністративно-правові акти щодо цього можна поділити на чотири категорії:

1) Конституція України та відповідні закони, що регулюють питання у цій сфері;

2) міжнародно-правові акти, згода на обов'язковість яких надана Верховною Радою України. Наприклад, конвенція Рада Європи «Про кіберзлочинність» 2001 р.;

3) нормативно-правові акти органів управління;

4) нормативно-правові акти спеціальних суб'єктів мережевої безпеки.

Як вказано в науковій літературі, що присвячена даній проблематиці, кібербезпека – це безпека інформаційних систем (апаратного та програмного забезпечення). Замість цього Інформаційна безпека – це безпека інформації, як правило, організації або компанії, в тому числі інформаційно-телекомунікаційні системи. Тому кібербезпека є частиною інформаційної безпеки, безпека для будь-якої організації.

Президент України 7 листопада 2017 року підписав Закон України «Про основні засади забезпечення кібербезпеки України», ухвалений Верховною Радою на початку жовтня. Текст документу було офіційно оприлюднено і, відповідно до його Перехідних положень, Закон набрав чинності 9 травня 2018 року [1].

Новий закон визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, а також основні засади координації їхньої діяльності із забезпечення кібербезпеки. Зокрема, Закон передбачає, що до суб'єктів національної системи кібербезпеки належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України, які будуть протидіяти кіберзагрозам в рамках повноважень, визначених цим Законом.

Важливо відзначити, що сфера регулювання Закону не поширюється на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, а також на соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів. Таким чином, принаймні формально, державні органи у сфері кібербезпеки не будуть втручатись у зміст оприлюдненої інформації, хоча виняток щодо «інформації, необхідність захисту якої встановлена законом» є досить широким і створює певні ризики [1].

Так, кіберпростір – це середовище (віртуальний простір), яке надає можливості реалізації комунікацій та/або реалізація соціальних відносин завдяки сумісним функціям (з'єднання) систем зв'язку та використання мереж для забезпечення електронного зв'язку інтернет та/або інші глобальні мережі передачі даних.

В січні 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України з урахуванням викликів, які стоять перед нашою державою: агресивних дій російської федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом [2].

Стратегія передбачає розвиток національної системи забезпечення захисту кіберпростору, своєчасного виявлення та нейтралізації кіберзагроз, а також запобігання їм з урахуванням досвіду та практики країн НАТО і Євросоюзу. Крім того, в документі обговорені питання координації, взаємодії та розподілу повноважень між органами безпеки та оборони України у питаннях кібербезпеки, кіберзахисту та протидії кіберзлочинності. Метою стратегії є створення умов для безпечного функціонування кіберпростору, його викори-

стання в інтересах особистості, суспільства і держави. В документі підкреслюється, що поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, вони можуть використовуватися для вчинення терористичних актів, у тому числі шляхом порушення штатних режимів роботи автоматизованих систем управління технологічними процесами на об'єктах інфраструктури. Більше поширення одержує політично мотивована діяльність у кіберпросторі у вигляді атак на урядові і приватні сайти в мережі Інтернет. "Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб в кіберпросторі. Цьому сприяє широке, іноді домінуюче, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо або побічно пов'язані з російською федерацією", - йдеться в концепції. [2, ст. 14-23]

Таким чином, в Україні діє цілий ряд органів державної влади і управління, покликаних забезпечувати реалізацію інформаційної функції. Необхідною умовою функціонування цих суб'єктів кібернетичної безпеки як узгодженої системи є, зокрема, належне нормативне правове регулювання.

Література:

1. Про основні засади забезпечення кібербезпеки України: закон України від 19.06.2015 р. Режим доступу: <http://zakon2.rada.gov.ua>
2. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України: указ Президента України від 27 січня 2016 року № 96/2016. Режим доступу: <http://zakon1.rada.gov.ua>. – Назва з екрану

ЗМІСТ

ВСТУПНЕ СЛОВО	3
---------------------	---

СЕКЦІЯ 1. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Андрій ШУЛЬГА ПРАВОНАЧУЩА ДИСТАНЦІЙНА ДІЯ: ПОНЯТТЯ, ОЗНАКИ.	5
Kseniya YURTAYEVA CYBERAGGRESSION AS A PART OF HYBRID WAR AGAINST UKRAINE.....	8
Карина МУКОЦА, Ганна ФОРОС ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ.....	11
Володимир ПЯДИШЕВ РОЗВИТОК КІБЕРЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР ДЕРЖАВ – НАГАЛЬНА ПРОБЛЕМА СУЧАСНОСТІ	13
Маріна АНДОНІЙ, Ганна ФОРОС ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ.	17
Вадим СУБОТКА, Надія МЕДВЕДЕНКО ПРАВОВЕ РЕГУЛЮВАННЯ ТА СУБ'ЄКТИ КІБЕРБЕЗПЕКИ В УКРАЇНІ.	19
Євгенія ФІЛАТОВА КІБЕРБЕЗПЕКА У ДЕРЖАВНОМУ СЕКТОРІ. ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ТРАНСПЛАНТАЦІЇ	22
Владислав ЛАСКАРЖЕВСЬКИЙ, Віталій СВІТЛИЧНИЙ КІБЕРАТАКИ: ПОНЯТТЯ ТА РЕАЛІЗАЦІЯ АТАК В КІБЕРПРОСТОРІ. DDOS-АТАКИ.....	25
Станіслав ЛАТИШЕВ, Віталій СВІТЛИЧНИЙ ДЕЯКІ ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ	26
Людмила РОТАРЬ, Ганна ФОРОС ОКРЕМІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ	28
Вікторія ТОМІНА, Данило ЗЕМЦЕВ ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА: ПРІОРИТЕТНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ В УМОВАХ ВОЄННОГО СТАНУ	30