

**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

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Ксенія КОЛОМІЄЦЬ

курсантка 302 навчального взводу

3 курсу ФПФПКП

Ганна ФОРОС

т.в.о. завідувача кафедри кібербезпеки та

інформаційного забезпечення ОДУВС,

к.ю.н., доцент

Інформаційна безпека та захист від кіберзагроз набуває особливої важливості в умовах війни. Крім цього, актуальність адміністративно-правового забезпечення кібербезпеки визначається сучасним розвитком інформаційного суспільства, який переходить від традиційного публічного адміністрування до урядування через електронні форми.

Розвиток інформаційного суспільства та сформовані правові інструменти забезпечують реалізацію інформаційних прав і обов'язків громадян, визначають ступінь розвитку інформаційної сфери України, стан інформаційного правопорядку, рівень забезпечення правової охорони і захисту соціальних цінностей [1].

Однак аналіз інформаційних законів свідчить про наявність істотних прогалин. Так, нині в законодавстві відсутня дефініція «інформаційна безпека», незважаючи на те, що це поняття дуже часто згадується в законодавстві. Наприклад, у Законі України «Про інформацію» міститься лише закріплення поняття «інформація» та «захист інформації» [2].

М.П. Ільницький влучно зазначає про те, що законодавцями у Законі України «Про інформацію» неповною мірою враховано всі можливі ризики нанесення шкоди інформаційній безпеці у сфері державного управління. З таким твердженням важко не погодитися, оскільки зміст закону складають в основному прості та бланкетні норми [3, 83].

Більше того, професор Р.А. Колужний зазначає, що невирішеними залишаються питання щодо термінологічної некоректності визначеності таких термінів, як «таємна інформація» і «таємниця», «документ» і «документована інформація», «майно», «власність», «володіння», «автоматизована система», «суб'єкт суспільних відносин» і «учасники суспільних відносин», «система інформаційних відносин» [4, 5–12].

Незважаючи на те, що в Україні упродовж останніх років існує багато законодавчих актів, які регулюють відносини, що виникають в інформаційній сфері, зокрема щодо забезпечення інформаційної безпеки держави, однак, у сучасних умовах розвитку суспільства інформаційне законодавство потребує певних якісних змін. На жаль, до цих пір воно залишається суперечливим, належним чином не систематизованим і не кодифікованим [5, с. 76].

Законодавство у сфері забезпечення кібербезпеки складається із сукупності норм адміністративно-правового регулювання, якими і забезпечується відповідний порядок у діяльності суб'єктів забезпечення кібербезпеки в Україні. Наприклад, статтею 8 Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що «національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [6].

Задля створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, 1 лютого 2022 року Президент України підписав указ про введення в дію рішення РНБО про «Про План реалізації Стратегії кібербезпеки України» [7].

Взагалі Стратегія кібербезпеки України (Стратегія) – це документ довгострокового планування, що встановлює пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування механізму протидії кіберзагрозам.

Стратегія 2021 року визначає три пріоритети: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки.

Крім цього, Стратегією визначено наступні цілі: 1) Дієва кібероборона. Для цього в структурі Міноборони заплановане створення кібервійська в першому півріччі 2023 року; 2) Протидія розвідувально-підбивній діяльності та кібертероризму; 3) Протидія кіберзлочинності шляхом завершення імплементації в українське законодавство положень Конвенції про кіберзлочинність та залучення відповідних практик США; 4) Розвиток асиметричних інструментів стримування; 5) Національна кіберготовність та надійний кіберзахист (таким чином документ обіцяє створення національної системи управління інцидентами); 6) Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки; 7) Безпечні цифрові послуги; 8) Зміцнення системи координації; 9) Формування нової моделі відносин у сфері кібербезпеки, де за державою закріплюватиметься роль партнера; 10) Прагматичне міжнародне співробітництво [7].

Таким чином, в умовах інформаційної війни слід приділяти максимальні зусилля для того, що уникнути частих кібер-атак, витоків інформації та інших кіберзагроз з боку російської федерації. Складністю є те, що діяльність російських хакерів із початком війни поступово трансформується. Наприклад, якщо в січні-березні 2022 року кібератаки були спрямовані на комунікації систем державного та військового управління, то після перших невдач на фронті агресор частково змінив вектор дій і сконцентрував зусилля на завданні шкоди цивільному населенню та об'єктам життєзабезпечення. Саме тому слід швидко реагувати на нові виклики, розробляти нові засоби протидії та втілювати їх в реальність.

Література:

1. Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07. Одеський державний університет внутрішніх справ. Одеса, 2021.
2. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-ХІІ. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650.
3. Ільницький М.П. Правове забезпечення інформаційної безпеки у сфері державного управління. *Науковий вісник Ужгородського національного університету*, Серія ПРАВО. 2015. Вип. 34, Т. 2. С. 83–87.

4. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4(24). С. 5–12.
5. Мороз Н. С. Законодавче регулювання інформаційної сфери як основа забезпечення інформаційної безпеки держави. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2015. № 824. С. 71-76.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.
7. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни. Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021

СЕКЦІЯ 2. АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Олександр МИКОЛЕНКО, Олена МИКОЛЕНКО РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА В ПУБЛІЧНО-ПРАВОВІЙ СФЕРІ	33
Ганна ФОРОС РЕЖИМ СЛУЖБОВОЇ ТАЄМНИЦІ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	37
Юлія ЛОБАНЬ, Ганна ФОРОС ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРНИТИЧНОЇ БЕЗПЕКИ	39
Каріна КОЛОМІЄЦЬ, Ганна ФОРОС АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗ-ПЕКИ В УКРАЇНІ	41

СЕКЦІЯ 3. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТБІ ЗІ ЗЛОЧИННІСТЮ

Олександр МОЖАСЬВ, Павло БУСЛОВ, Юрій ГНУСОВ ІНФОРМАЦІЙНА МОДЕЛЬ ФОРМУВАННЯ СОЦІАЛЬНОГО ПРОФІЛЮ ОСОБИСТОСТІ НА ОСНОВІ ТЕХНОЛОГІЇ OSINT	45
Susan M. LAWLOR VISION OF MODERN LAW ENFORCEMENT	47
Микита ШЕВЧЕНКО, Віталій СВІТЛИЧНИЙ ЗЛОЧИННІСТЬ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ	50
Francesco PANEBIANCO CYBERSECURITY WITHIN EU STRATEGIC PRIORITIES: PROTECTING EVERYONE IN THE EU	53
Роман БОРМАТОВ, Віталій СВІТЛИЧНИЙ КІБЕРЗЛОЧИНИ У ФІНАНСОВО-БАНКІВСЬКІЙ СФЕРІ, СКІМІНГ	55
Олексій БАЛТОВСЬКИЙ, Олександр ГЕРАСИМЕНКО ІНСТРУМЕНТАРІЙ РОЗВ'ЯЗАННЯ ОПТИМІЗАЦІЙНИХ ЗАДАЧ ДЕКОМПЗИЦІЇ ФУНКЦІОНАЛЬНИХ АЛГОРИТМІВ АДАПТИВНОЇ СПІР ДЛЯ ПРОЕКТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖИ	57