

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
17 листопада 2023 року**

Одеса
ОДУВС
2023

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: матеріали міжн.
наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. --
- 168 с.

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 17 листопада 2023 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, 2023

основною інформацією та статистикою (тобто звітом CompStat), а конкретні питання щодо злочину могли ставились особі, яка несла безпосередню відповідальність за стан злочинності в територіальному відділенні поліції – його керівнику. Начальник територіального відділення поліції міг відповідати безпосередньо і публічно вищому керівнику, що ставить питання, таким чином створювалася атмосфера прозорості та справедливості, тому що всі учасники наради мали одну й ту саму інформацію, і дотримувалися одного стандарту.

Для підвищення соціальної відповідальності адміністрації за використання технологій CompStat застосовується принцип забезпечення прозорості. Поліція Нью-Йорка публікує деякі дані, включаючи вдосконалені за допомогою програми CompStat звіти для кожної зони та міста в цілому, на своєму веб-сайті.

Модель комп'ютерної статистичної поліцейської діяльності (CompStat) – це система управління, у якій розробляється модель, за якою незначні злочини розглядаються як елемент зменшення більш тяжких. На підставі аналізу статистики вже вчинених злочинів окремі регіональні керівники правоохоронних органів є відповідальними за впровадження на місцевому рівні заходів, які вже завчасно розроблені. CompStat концентрується в основному на вуличних і серійних злочинах із забезпеченням короткострокової підзвітності в процесі вирішення нових кримінальних викликів. Варіанти програми CompStat використовуються в поліцейських дільницях по всьому світу.

Література:

1. Carter J.G., Phillips S.W., Gayadeen S.M. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. Journal of Criminal Justice . 2014. № 42. P. 433–442.
2. Користін О. Є., Пефтієв Д. О., Некрасов В. А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою/ILP : навчальний посібник / за заг. ред. М.Г. Вербенського. К., 2019. 120 с.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕЗЛОЧИННОСТІ СПІВРОБІТНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Форос Ганна Володимирівна

кандидат юридичних наук, доцент
завідувачка кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ,

Шимко Діана Сергіївна

слухачка I курсу магістратури ФПФОДР
Одеський державний університет внутрішніх справ

Зв'язок через електронні засоби став основою для банків, авіакомпаній та корпорацій, утримуючи їхню стабільність. Проте, кіберзлочинці не обов'язково діють на вулицях: студенти та підлітки з ноутбуками та доступом до мережі можуть стати злочинцями. У військових конфліктах вони перетворюються на інформаційних воїнів, використовуючи кібератаки та злам для ефективних атак.

Під час військового конфлікту в Україні кібератаки шахраїв, які намагаються незаконно заволодіти коштами через Інтернет, завдають значної шкоди, подібно до руйнування на полі бою. Статистика показує, що виявлені випадки кіберзлочинів зростали майже в 7,5 рази від 1998 по 2021 рік, без врахування класичних комп'ютерних правопорушень та рівня прихованості. У період війни кількість кіберпроступків зросла вдвічі. Це створює гостру потребу в оптимізації роботи правоохоронних органів, особливо в умовах поширення багатой дезінформації, що потребує швидкого реагування на фейки й ефективного протидії кіберзлочинцям, особливо в соціальних мережах [1].

Закон України, який регулює основні аспекти забезпечення кібербезпеки, а саме: Закон України «Про основні засади забезпечення кібербезпеки України», визначає кібербезпеку як захист важливих інтересів людини, суспільства і держави в онлайн просторі. Це забезпечує сталий розвиток інформаційного суспільства і цифрового середовища, а також вчасне виявлення, запобігання та припинення потенційних загроз для національної.

Упереджено в Законі України "Про основні засади забезпечення кібербезпеки України", Національна поліція України є однією з основних складових національної системи кібербезпеки, що активно формується відповідно до глобальних тенденцій у сфері кіберзахисту. Від концептуального визначення до практичного запровадження, ця система виступає вирішальним фактором, який є необхідним для забезпечення захищеності життєво важливих інтересів людини, громадянина, суспільства і держави під час користування кіберпростором.

За словами М.М. Присяжнюка та Є.І. Цифри, в Україні виникає необхідність у створенні ефективної системи безпеки в умовах, коли виклики, що ставлять під загрозу національну безпеку, набувають нових форм, відмінних від традиційних загроз. Зростання активності провідних держав у кіберпросторі, значні зміни у підходах до внутрішньої інформаційної політики, а також формування міцних транснаціональних злочинних груп, спеціалізованих на кіберзлочинах, підкреслюють важливість розробки рекомендацій для трансформації вітчизняного сектора безпеки у коротко- та довгострокові пріоритети [3, с. 65].

Оскільки національна система безпеки включає багато складових, В.А. Ліпкан і І.В. Діордіца висловлюють необхідність наявності окремої підсистеми, що спрямована на забезпечення функціонування та розвитку цієї системи. Основна мета цієї підсистеми полягає у підтримці життєздатності різних складових цієї системи, зокрема національних інтересів людини, суспільства та держави. Дослідники висвітлюють аспекти системи забезпечення національної безпеки та національної системи кібербезпеки, звертаючи увагу на відмінності в підходах до формування цих категорій [4, с. 174].

Пригадуючи компоненти національної системи кібербезпеки України, визначені в даний час у Законі України "Про основні засади забезпечення кібербезпеки України", важливо зауважити, що всі названі основні учасники належать до органів держави: 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 [2].

Роль вказаних учасників у забезпеченні кібербезпеки наростає, проте поки не йдеться про те, наскільки ефективно вони взаємодіють. Після ретельного адміністративно-правового аналізу регулювання кібербезпеки в Україні, І.В. Діордіца вказує на те, що кібернетична функція держави, через свою властиву організаційну природу, повинна бути реалізована через створення ефективної національної системи кібербезпеки, залучаючи всі центральні органи виконавчої влади, а також недержавні, включаючи волонтерські організації, кожного окремого учасника правовідносин у сфері кібербезпеки [5, с. 11]. Однією з ключових аспектів ефективної організації роботи національних систем кібербезпеки науковець визначає установлення взаємодії між компетентними державними органами, які є учасниками кібербезпеки, та координацію їхньої діяльності [4, с. 178-179].

У відповідності до українського законодавства, кіберзлочин (або комп'ютерний злочин) – це діяння, яке відбувається у кіберпросторі або за його використанням і є суспільно небезпечним, підлягаючи відповідальності відповідно до Кримінального кодексу України та/або міжнародних договорів України. Основною метою таких незаконних дій є руйнування або незаконне заволодіння інформацією в інформаційних системах [2].

Отже, законодавство визнало проблему кібератак у сфері інформаційного простору аналогічно до наслідків воєнних дій. Це призвело до внесення відповідних змін та доповнень до кримінального та адміністративного законодавства, ураховуючи при цьому міжнародне право. Ці зміни сприяли удосконаленню основ та процедур притягнення осіб до юридичної відповідальності. Зокрема, внесені доповнення до Законів України "Про Національну поліцію" та "Про внесення змін до Кримінального кодексу України для підвищення ефективності боротьби з кіберзлочинністю у період дії воєнного стану" від 24 березня 2022 року за №2149-IX. Рішення про посилення відповідальності за незаконні дії у кіберпросторі є важливим кроком [6].

Отже, аналіз законодавства та практики його застосування в діяльності Національної поліції в сфері кібербезпеки в Україні підтверджує, що ці підрозділи, крім заходів захисту інформації, активно використовують новітні технології для протидії комп'ютерній злочинності та кіберзагрозам. Однак у сучасних умовах також критично важливо розробити систему заходів, спрямованих на чітке визначення поняття "дезінформація" у цифровому просторі, а також методи її виявлення та протидії шляхом закріплення цих аспектів у законодавстві.

Література:

1. Боротьба з кіберзлочинністю в умовах воєнного стану. URL: https://jurliga.ligazakon.net/analytys/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanuzakon-2149-ix (дата звернення: 10.11.2023).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. № 2163-VIII. Відомості Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 10.11.2023).
3. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. Реєстрація, зберігання і обробка даних. 2017. Т. 19. № 2. С. 61–68. (дата звернення: 10.11.2023).
4. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174–180. (дата звернення: 10.11.2023).
5. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.0; Запорізький нац. ун-т. Запоріжжя, 2018. 32 с. (дата звернення: 10.11.2023).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022. № 2149-IX. URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 10.11.2023).

ОСОБЛИВОСТІ ЗМІН КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИНИ В УКРАЇНІ

Лучик Василь Єфремович

доктор економічних наук

професор кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутрішніх справ

Кочин Владислав Дмитрович

Здобувач вищої освіти

З самого початку існування України, як незалежної держави, влада незалежної України боролася із кіберзлочинністю. Аналізуючи [1-3], можна визначити власне поняття кіберзлочину. Кіберзлочин – небезпечні та незаконні діяння, які спрямовані на кіберпростір за допомогою електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж і мереж електрозв'язку.

Згідно конвенції Ради Європи по боротьбі з кіберзлочинністю виділяють 4 основних типи кіберзлочинів:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- злочини щодо авторських і суміжних прав;
- шахрайство та підробка, пов'язані з використанням комп'ютерів;
- злочини, пов'язані з розміщенням у мережах протиправної інформації

[2].

У свою чергу, Рада Європи по боротьбі з кіберзлочинністю [3] ділить кіберзлочини на 10 видів: піратство, скімінг, кардинг, фішинг, вішинг, шимінг, рефайлінг, мальваре, протиправний контент, онлайн-шахрайство.

Україна почала боротися із кіберзлочинністю ще з 2001 року, і відповідальність за кіберзлочини з'явилася у XVI розділі Кримінального кодексу України під назвою

ШЛЯХИ УДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ ДОКТРИНИ КІБЕРБЕЗПЕКИ	26
<i>Безуглий Леонід Анатолійович</i> - кандидат юридичних наук, головний спеціаліст відділу координації первинної професійної підготовки та професійного навчання Управління освітньої діяльності Департаменту освіти, науки та спорту МВС	
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЇХ ПРОБЛЕМАТИКА	29
<i>Форос Ганна Володимирівна</i> - кандидат юридичних наук, доцент, завідувачка кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ,	
<i>Вівіровський Михайло</i> - курсант 3 курсу ФПФODP Одеський державний університет внутрішніх справ	
АНАЛІЗ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ОПЕРАТИВНОГО МОНІТОРИНГУ ТА СКЛАДНОГО УПРАВЛІННЯ ПОДІЯМИ В ГАЛУЗІ БЕЗПЕКИ	31
<i>Балтовський Олексій Анатолійович</i> - доктор технічних наук, доцент, професор кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД В УМОВАХ ВОЄННОГО СТАНУ	33
<i>Мельнікова Олена Олександрівна</i> - кандидат юридичних наук, доцент, викладач кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
СТРУКТУРА КОМПЕТЕНТНОСТІ ЮРИСТІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ	25
<i>Онищенко Денис Рафетович</i> - слухач 2 курсу магістратури ІПБ, спеціальність 124 «Системний аналіз» Одеський державний університет внутрішніх справ	
<i>Мельнікова Олена Олександрівна</i> - кандидат юридичних наук, доцент, викладач кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
ОПТИМІЗАЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ В КОНТЕКСТІ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ	36
<i>Прохорчук Євген Олександрович</i> - слухач 2 курсу магістратури ІПБ, спеціальність 124 «Системний аналіз» Одеський державний університет внутрішніх справ	
<i>Мельнікова Олена Олександрівна</i> - кандидат юридичних наук, доцент, викладач кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
ОСНОВНІ НАПРЯМИ РОЗВИТКУ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ	38
<i>Калугін Володимир Юрійович</i> - кандидат юридичних наук, доцент, професор кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
<i>Бовтенко Денис Геннадійович</i> - слухач 2 курсу магістратури ІПБ, спеціальність 124 «Системний аналіз» Одеський державний університет внутрішніх справ	
ВИКОРИСТАННЯ ПРОГРАМИ КОМП'ЮТЕРИЗАЦІЇ COMPSTAT У ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ УПРАВЛІНЬ США	39
<i>Тодоров Василь Іванович</i> - слухач 2 курсу магістратури ІПБ, спеціальність 124 «Системний аналіз» Одеський державний університет внутрішніх справ	
<i>Мельнікова Олена Олександрівна</i> - кандидат юридичних наук, доцент, викладач кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ СПІВРОБІТНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ	41
<i>Форос Ганна Володимирівна</i> - кандидат юридичних наук, доцент, завідувачка кафедри кібербезпеки та інформаційного забезпечення Одеський державний університет внутрішніх справ	
<i>Шимко Діана Сергіївна</i> - слухачка 1 курсу магістратури ФПФODP Одеський державний університет внутрішніх справ	
ОСОБЛИВОСТІ ЗМІН КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИННИ В УКРАЇНІ	43
<i>Лучик Василь Єфремович</i> - доктор економічних наук, професор кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ	
<i>Кочин Владислав Дмитрович</i> - здобувач вищої освіти	
ЗАСТОСУВАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ФІКСАЦІЇ ВОЄННИХ ЗЛОЧИНІВ	45
<i>Лучик Світлана Дмитрівна</i> - доктор економічних наук, професор, професор кафедри протидії кіберзлочинності Харківський національний університет внутрішніх справ	
<i>Столик Денис</i> - курсант спеціальності «Кібербезпека», Харківський національний університет внутрішніх справ	
ПИТАННЯ ДОКАЗУВАННЯ В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ЩОДО ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ, СПРЯМОВАНОЇ НА УХИЛЕННЯ ВІД СПЛАТИ ПОДАТКІВ, ЗБОРІВ (ОБОВ'ЯЗКОВИХ ПЛАТЕЖІВ)	47
<i>Григорашенко Олександр Вікторович</i> - аспірант Одеського державного університету внутрішніх справ	