

МВС України  
Харківський національний університет  
внутрішніх справ  
Координатор проектів ОБСЄ в Україні

# **ПРОТИДІЯ КІБЕРЗАГРОЗАМ ТА ТОРГІВЛІ ЛЮДЬМИ**

**Збірник матеріалів  
Міжнародної науково-практичної конференції**

**(26 листопада 2019 року, м. Харків)**

Харків  
ХНУВС  
2019

УДК [351.74:343.85](062.552)

П83

*Друкується згідно з рішенням оргкомітету  
за дорученнями Харківського національного університету внутрішніх  
справ від 17.09.2019 № 125*

П83 Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2019. – 330 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

**УДК [351.74:343.85](062.552)**

*Публікації наведено в авторській редакції.*

*Оргкомітет не завжди поділяє погляди авторів публікацій.*

*За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних імен, географічних назв, а також за розголошення фактів, що не підлягають відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.*

*Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (<http://www.univd.edu.ua>) у розділі «Видавнича діяльність. Матеріали науково-практичних конференцій, семінарів тощо», а також у репозитарії ХНУВС (<http://dspace.univd.edu.ua/xmlui/>).*

Видано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», за фінансової підтримки уряду Сполучених Штатів Америки.

Усі права захищено. Зміст посібника можна безкоштовно копіювати та використовувати в освітніх та інших некомерційних цілях за умови посилання на джерело інформації.

**Координатор проектів ОБСЄ в Україні на уряд Сполучених Штатів Америки не несуть відповідальність за зміст та погляди, висловлені у цій публікації.**

© Харківський національний університет внутрішніх справ, 2019

© Координатор проектів ОБСЄ в Україні, 2019

# ЗМІСТ

---

## Розділ 1 Окремі питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми

---

### **Швець Д.В.**

Механізми забезпечення кібербезпеки в інформаційному просторі. . . 14

### **Авдєєва Г.К.**

Проблеми застосування інноваційних продуктів у протидії  
кіберзагрозам . . . . . 18

### **Балаклієць А.О., Калиновський О.В.**

Проблема торгівлі людьми в Україні . . . . . 21

### **Балик В.Р.**

Кіберзлочинність: правові аспекти та механізми забезпечення  
протидії. . . . . 26

### **Бандурка О.М.**

Окремі напрями взаємодії Харківського національного  
університету внутрішніх справ з територіальними органами  
Національної поліції щодо протидії технологічним наркозлочинам . 29

### **Батог А.Г., Шевченко А.Л.**

Право на інтернет як фундаментальне право людини . . . . . 31

### **Бортник С.М.**

Соціальна інженерія як метод вчинення злочинів. . . . . 34

### **Бортнік П.Р., Воєводін І.С.**

Правова природа та сутність кіберзлочинності. . . . . 36

### **Бурдін М.Ю.**

Кримінальний аналіз у роботі оперативних підрозділів  
Національної поліції України . . . . . 39

### **Ведернікова А.О.**

Необхідність кримінально-правового регулювання кібербулінгу . . . 42

<b>Воєводін І.С.</b>	
Кібервійна як сучасний метод ведення збройних конфліктів . . . . .	46
<b>Гурзель Ю.В.</b>	
Кіберзлочинність: основні причини та методи боротьби . . . . .	49
<b>Войціховський А.В.</b>	
Кібератаки як елемент гібридної війни . . . . .	52
<b>Гладкий В.В.</b>	
Корупційна толерантність до торгівлі людьми . . . . .	55
<b>Герасимюк В.С., Онищенко Ю.М.</b>	
Проблеми забезпечення кібербезпеки як складової публічної безпеки . . . . .	58
<b>Гнусов Ю.В., Калякін С.В.</b>	
Кримінальний аналіз у роботі підрозділів Національної поліції України . . . . .	61
<b>Головко О.М.</b>	
Кіберзлочини та парадигма Human Rights . . . . .	64
<b>Градова Ю.В.</b>	
Кібербулінг як загроза психологічному здоров'ю підлітків. . . . .	66
<b>Григорчак Я.О.</b>	
Щодо ролі засобів масової інформації у протидії торгівлі людьми . . . . .	69
<b>Єрошкін М.В.</b>	
Заборона насильницьких зникнень в Україні . . . . .	71
<b>Іващенко В.О.</b>	
Окремі аспекти нормативно-правового забезпечення протидії торгівлі людьми . . . . .	73
<b>Івасечко Р.А.</b>	
Кіберзлочинність як один із найбільш прогресивних видів злочинів сучасності. . . . .	76
<b>Калініна А.В.</b>	
Криптовалюта – «цифровий актив» злочинності? . . . . .	79
<b>Maryana Kachynska</b>	
Developing a labor perspective to human trafficking in the political-economic context of ukraine . . . . .	83

<b>Ковтун В.О.</b>	
Протидія кібербулінгу як сучасній формі агресії . . . . .	86
<b>Коженівський Т.В.</b>	
Кіберзлочинність як загроза сучасній безпеці . . . . .	89
<b>Коломоєць К.С., Тітов Є.Б.</b>	
Незаконне розповсюдження наркотичних речовин через мережу інтернет як загроза правопорядку . . . . .	93
<b>Кравчук С.М.</b>	
Теоретико-правові дослідження торгівлі людьми як підґрунтя для її подолання . . . . .	96
<b>Коротков І.С.</b>	
Протидія торгівлі людьми в інформаційній сфері . . . . .	99
<b>Макаренко П.В., Доценко В.В.</b>	
Психологічні аспекти протидії гендерному насильству . . . . .	101
<b>Лисак В.Р.</b>	
Кіберзлочинність: як захистити себе в мережі . . . . .	106
<b>Марков В.В., Фролова Т.А.</b>	
Манипуляція інформацією как метод інформаційного тероризма и інформаційної війни . . . . .	109
<b>Марчук М.І.</b>	
Право на інтернет як базове право людини . . . . .	116
<b>Мовчан А.В.</b>	
Окремі аспекти протидії кіберзлочинності підрозділами кіберполіції Національної поліції України . . . . .	120
<b>Онищенко Ю.М., Шарабан О.І.</b>	
Сучасні інструменти аналітичної роботи для підрозділів Національної поліції України . . . . .	123
<b>Осятинська І.А.</b>	
Напрями роботи з потерпілими від злочинів, пов'язаних з торгівлею людьми . . . . .	125
<b>Печора К.В.</b>	
Нормативно-правові засади діяльності Національної поліції України у сфері протидії торгівлі людьми . . . . .	127

<b>Расторгуєва Н.О., Загуменна Ю.О.</b>	
Діджиталізація сучасного суспільства . . . . .	130
<b>Серватовський А.В., Онищенко Ю.М.</b>	
Легалізація (відмивання) доходів, одержаних злочинним шляхом, за допомогою криптовалют . . . . .	133
<b>Сокурєнко В.В.</b>	
Комплексний підхід до вирішення питання кібербезпеки України .	135
<b>Стець А.М.</b>	
Онлайн-шахрайство та його небезпека . . . . .	138
<b>Струков В.М., Узлов Д.Ю., Пірієв А.О.</b>	
Сучасні високотехнологічні тренди у кримінальному світі . . . . .	141
<b>Чалабієва М.Р.</b>	
Дезінформація в електронних засобах масової інформації . . . . .	145
<b>Шевчук Т.А.</b>	
Розповсюдження наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет . . . . .	147

**Розділ 2**  
**Кримінально-правові, процесуальні та криміналістичні аспекти протидії кіберзлочинності та торгівлі людьми**

---

<b>Батиргарєєва В.С.</b>	
Сучасний віктимологічний портрет потерпілої особи від торгівлі людьми . . . . .	152
<b>Бабій Н.Р., Бурак М.В.</b>	
Отримання інформації про факти торгівлі людьми . . . . .	155
<b>Давидюк В.М.</b>	
Сучасні тенденції в роботі з конфідентами . . . . .	158
<b>Загуменний О.О.</b>	
Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини» . . . . .	160

<b>Золотарьов С.О.</b>	
Дослідження розумних годинників . . . . .	164
<b>Казначєєва Д.В.</b>	
Основні види злочинів, що вчиняються із застосуванням криптовалюти . . . . .	166
<b>Коваленко І.О., Єфімов М.М.</b>	
До питання протидії шахрайству у сфері використання банківських електронних платежів. . . . .	169
<b>Лєсь І.О.</b>	
Характерні ознаки жертви дитячої порнографії . . . . .	172
<b>Макаров В.С.</b>	
Новітні технології в комп'ютерно-технічній експертизі: дослідження дронів . . . . .	175
<b>Манжай О.В.</b>	
Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів . . . . .	178
<b>Мітрухов П.М.</b>	
Шляхи вирішення окремих проблем роботи слідчо-оперативної групи . . . . .	181
<b>Мурадлі А.</b>	
Криміналістична характеристика торговців людьми. . . . .	185
<b>Орлов Р.Р., Євтушок В.А.</b>	
Застосування поліграфа в діяльності поліції. . . . .	188
<b>Орлов Р.Р., Онищенко Ю.М.</b>	
Web-сервери: безпека використання та застосування . . . . .	190
<b>Панасюк І.В.</b>	
Робота з великими текстовими масивами у правоохоронних органах . . . . .	192
<b>Пилипенко О.В.</b>	
Методи фіксації інформації вебсайтів, які можуть бути використані в комп'ютерно-технічній експертизі . . . . .	194
<b>Політова А.С.</b>	
Детермінанти торгівлі людьми. . . . .	197

<b>Рог В.Е., Мелашенко О.П., Лебедєв Д.</b>	
Следообразование при неправомерном доступе к компьютерной системе или сети . . . . .	200
<b>Сапужак С.М.</b>	
Кіберзлочинність: характеристика поняття та способи захисту . . . . .	203

### Розділ 3

#### Використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми

---

<b>Барбашов О.Г., Грищенко Д.О.</b>	
Щодо заходів безпеки для запобігання кіберзлочинності. . . . .	208
<b>Рвачов О.М., Лактіонов В.В., Дацюк Д.О.</b>	
Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет. . . . .	210
<b>Бичков С.О.</b>	
Штатні засоби криптографічного захисту інформації користувача в операційних системах Microsoft Windows та MAC OS . . . . .	218
<b>Белік Д.С., Цуранов М.В.</b>	
Методи боротьби з кібершахраями в магазинах цифрової дистрибуції . . . . .	221
<b>Воронько В.О., Цуранов М.В.</b>	
Біометрична ідентифікація як захист від несанкціонованого доступу . . . . .	224
<b>David A., Horelov Y., Horelov O.</b>	
Some aspects of security in adaptive systems of distance learning. . . . .	227
<b>Дука І.О., Певнєв В.Я.</b>	
Способи виявлення таємних комунікацій кіберзлочинців . . . . .	230
<b>Клімушин П.С., Колісник Т.П.</b>	
Безпека національної інфраструктури електронних підписів . . . . .	233
<b>Клімушин П.С., Білобров А.В.</b>	
Криптологія як провідний метод захисту інформації в сучасному суспільстві. . . . .	236

<b>Кобзев І.В., Петрова К.К.</b>	
Кібербезпека та відкриті дані . . . . .	240
<b>Казмірчук І.С., Євтушок В.А.</b>	
Штучні нейронні мережі, їх використання у кіберзлочинності та боротьбі з нею . . . . .	243
<b>Коршенко В.А.</b>	
Гаджети – прихована загроза . . . . .	245
<b>Мордвинцев М.В., Хлестков О.В., Ницюк С.П.</b>	
Стан і перспективи розвитку інформаційно-аналітичних систем для вирішення завдань правоохоронних органів . . . . .	248
<b>Ведмідь М.А.</b>	
Аналіз методів захисту інтернет- і мобільного банкінгу. . . . .	251
<b>Єременко М.А.</b>	
Метод двофакторної автентифікації як засіб боротьби з шахраями в мережі інтернет . . . . .	255
<b>Лоцман Є.Р.</b>	
Методи деанонізації як засіб виявлення правопорушників . . . . .	259
<b>Можаяєв О.О., Наєм Х.Р.</b>	
Метод розподілу мережного ресурсу гібридної комп'ютерної геоінформаційної мережі МВС України з використанням технології МІМО . . . . .	262
<b>Семенов С.Г., Волошин Д.Г., Давидов В.В.</b>	
GERT-мережа виконання польотного завдання БПЛА в умовах зовнішніх впливів. . . . .	264
<b>Семенов С.Г., Мелешко Є.В., Рашидінія А.</b>	
Аналіз характеристик безпеки рекомендаційних систем і вдосконалення моделі прогнозування змін подоби їх користувачів . . . . .	266
<b>Семенова А.С., Бартош М.В., Сиротенко М.Є.</b>	
Прогнозування часових витрат на розробку безпечного програмного забезпечення . . . . .	268
<b>Сергієнко В.М., Шипова Т.М., Можаяєв М.О.</b>	
Розробка протоколів розподілу доступу для захисту даних на основі можливих сценаріїв роботи системи обробки й управління запитами . . . . .	269

<b>Світличний В.А.</b>	
Вразливість операційної системи Android . . . . .	271
<b>Chuhai A.M., Shekhovtsov S.B., Diaz R.C.</b>	
Application of parallel calculations in large scale optimization problems	273
<b>Халіфе К.</b>	
Удосконалений спосіб оцінки вразливості системного програмного забезпечення . . . . .	275
<b>Школьніков В.І.</b>	
Використання можливостей прикладного програмного інтерфейсу для аналізу криміналістичної інформації . . . . .	277
<b>Шорский О.Е., Певнев В.Я.</b>	
Антивірусний захист локальної мережі як засіб боротьби з правопорушеннями в кіберпросторі . . . . .	280

**Розділ 4**  
**Кадрове забезпечення протидії**  
**кіберзлочинності та торгівлі людьми**

---

<b>Манжай І.А.</b>	
Особливості використання web-квестів для навчання студентів. . .	284
<b>Носов В.В.</b>	
Гейміфіковане навчання кібербезпеки та цифрових криміналістичних досліджень у виші . . . . .	286
<b>Панова О.О.</b>	
Шляхи оптимізації кадрового забезпечення протидії торгівлі людьми . . . . .	289

## Розділ 5

### Міжнародний досвід протидії кіберзлочинності та торгівлі людьми

#### **Артамонова М.Г., Воєводін І.С.**

Сутнісна характеристика поняття та міжнародний досвід протидії кібермобінгу . . . . . 294

#### **Barbashov O.**

Foreign experience in combating cybercrime as exemplified by the USA and Japan . . . . . 297

#### **Бойко М.В., Тітов Є.Б.**

Діяльність інтерполу в боротьбі з кіберзлочинами . . . . . 299

#### **Варнавська К.А.**

Деякі питання захисту жінок-журналістів у мережі Інтернет: міжнародно-правовий аспект. . . . . 301

#### **Гудзь Т.І.**

Принцип вільного руху інформації як основний принцип європейської аудіовізуальної політики . . . . . 305

#### **Гусаров С.М.**

Міжнародна співпраця у сфері протидії кібертероризму . . . . . 309

#### **Євтушок В.А.**

Боротьба з торгівлею людьми на міжнародному рівні та її наслідки 311

#### **Оніщенко В.В.**

Деякі питання торгівлі людьми в бізнес-сфері: міжнародно-правовий аспект. . . . . 314

#### **Предибайло А.І.**

Міжнародно-правові механізми протидії торгівлі особами похилого віку. . . . . 317

#### **Перепелиця М.М.**

Зарубіжний досвід розшуку безвісти зниклих осіб . . . . . 320

#### **Сироїд Т.Л.**

Міжнародні спеціалізовані інституції у сфері протидії торгівлі людьми . . . . . 322

#### **Шевченко А.Л.**

Забезпечення інформаційної безпеки потерпілих персоналом Міжнародного кримінального суду . . . . . 326

**УДК 341.4:004**

**Андрій Васильович Войціховський,**

*кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ*

## **Кібератаки як елемент гібридної війни**

Гібридна війна може розглядатися як більш досконалий або ефективний спосіб ведення війни, оскільки вона прагне досягти політичних цілей без широкого використання збройних сил та насильства. Особливістю гібридної війни є свідоме розмиття меж між війною і миром, вона не оголошується, її ініціювання зазвичай проходить непомітно. Використання цілого ряду інструментів гібридної війни, таких як кібератаки, заходи економічного впливу, інформаційні операції та обмежені фізичні атаки, які породжують невизначеність у широких верств населення, можуть бути достатніми для досягнення політичних цілей.

Одним із ефективних елементів гібридної війни є кібератаки. Вони направлені, насамперед, на дестабілізацію комп'ютерних систем держави. Міждержавні відносини і політичне протистояння інколи знаходять своє продовження в мережі Інтернет у вигляді окремих проявів втручання в комп'ютерні системи. Розглянемо лише декілька видів кібератак, що є елементами гібридної війни:

- вандалізм – атака, яка завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат. До таких кібернетичних атак можна віднести пошкодження вебсайтів державних органів і установ, заміну змісту образливими чи пропагандистськими малюнками тощо;

- пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення;

- збір інформації (кібершпигунство) – злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні;

- відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких є порушення функціонування сайтів або комп'ютерних систем;

- втручання в роботу обладнання – атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем, що призведе до відключення або виникнення помилок при обміні даними;

- атаки на об'єкти критичної інфраструктури – атаки на комп'ютери та системи, що забезпечують життєдіяльність населених пунктів і держави взагалі, а саме: системи водопостачання, електроенергії, транспорту тощо [1].

З розвитком інформаційно-комунікаційних технологій рівень і чисельність кібератак постійно зростає. Деякі держави почали приділяти значну увагу захисту від кібератак – розробляти необхідні засоби для організації системної оборони і захисту об'єктів критичної інфраструктури, а також формувати спеціальні підрозділи, основним завданням яких є забезпечення національної кібербезпеки.

Крім того, держави почали витратити більше ресурсів на створення своїх кіберможливостей, і роль використання кібердомену (віртуальної сфери) неспинно зростає саме у військовій сфері. Такий стан речей свідчить про початок гонки цифрових озброєнь, де правила участі міжнародною спільнотою ще не кодифіковані.

Розвинені країни докладають значних зусиль для вироблення власної кібернетичної зброї, яка замінить за ефективністю класичну зброю (кулі, бомби, танки, літаки тощо). Такий сценарій розвитку військової стратегії вже стає реальністю. Так, наприклад, Міністерство оборони США відкрито заявляє, що вони створюють комп'ютерний код, здатний вбивати. Згідно з опублікованим посібником Міністерства оборони США про військові дії, операції із використанням кіберзброї можуть викликати такі загрози як знищення або пошкодження ядерної установки; відкриття дамби над населеним пунктом, що спричинить руйнування; відключення служби управління повітряним рухом, що спричинить аварії літаків тощо [2, с. 522].

У сучасних умовах розвитку інформаційного суспільства ефективна протидія кібератакам як проявам гібридної війни потребує не лише спільних зусиль розвинутих країн світу, але й розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав.

Забезпечення ефективної протидії кібератакам диктує важливість розробки, здійснення й удосконалення ефективних національних і міжнародних заходів:

- розробка державами ефективних моделей державної політики та національної концепції з кібербезпеки, що відповідають вимогам національної безпеки держав в контексті глобальних викликів та інших тенденцій сучасності;

- розвиток міжнародно-правових механізмів і загальної міжнародної політики по розробці і здійсненню ефективних інструментів з протидії кібератакам;

- налагодження і розвиток тісного співробітництва з НАТО, ОБСЄ, ЄС у галузі протидії різним проявам гібридної війти, у тому числі кібератака тощо.

#### **Список бібліографічних посилань**

1. Івахів Б. Кібертероризм як засіб ведення зовнішньої політики РФ // Free Voice Information Analysis Center : сайт. URL: <http://iac.org.ua/kiberterrorizm-yak-zasib-vedennya-zovnishnoyi-politiki-rf/> (дата звернення: 20.10.2017).
2. Кібербезпека як важлива складова всієї системи захисту держави // Міністерство оборони України : офіц. веб сайт. 07.05.2018. URL: <http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html> (дата звернення: 26.10.2019).
3. Linnell J. The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. 2015. Vol. 4, No. 4. P. 521–532. DOI: <https://doi.org/10.17781/P001973>.

*Одержано 28.10.2019*

*Наукове видання*

## ПРОТИДІЯ КІБЕРЗАГРОЗАМ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів  
Міжнародної науково-практичної конференції,  
(26 листопада 2019 року, м. Харків)

*Українською, англійською та російською мовами*

Відповідальні за випуск: *О. В. Манжай*  
Редактор: *О. В. Манжай*  
Корегування списків бібліографічних посилань: *О. В. Манжай,*  
*С. С. Тарасова, П. О. Білоус*  
Комп'ютерне верстання: *О. В. Манжай*

Формат 60x84 1/16. Ум. друк. арк. 11,24 Обл.-вид. арк. 12,4.  
Тираж 200 пр.