

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Прієшкіна О. В. Забезпечення прав людини в Україні: стан та перспективи. Наукові записки НаУКМА. 2017. Том 200. Юридичні науки С.110.
2. Конституція України 1996 р. URL: https://static.rada.gov.ua/NEWSAJT/site/const/pershe_chytannya_96.html
3. Кошель С. Які права можуть і не можуть бути обмежені під час воєнного стану. URL: <https://ldn.org.ua/consultations/yaki-prava-mozhut-i-ne-mozhut-butty-obmezheni-pid-chas-voiennoho-stanu/>
4. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції : Закон України від 17 липня 1997 р. // Відомості Верховної Ради України. – 1997. – № 40. – Ст. 263

**Піщенко Г. І., к.ю.н., доц.,
професор кафедри кримінального права
та кримінології,
Навчально-науковий інститут права та психології,
Національної академії внутрішніх справ,
м. Київ**

КІБЕРБЕЗПЕКА ТА КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: СУЧАСНИЙ СТАН

Кібербезпека – це комплексна діяльність, що використовує технології, процеси та методи для захисту комп'ютерних систем, мереж, програм та даних від кібератак, несанкціонованого доступу, пошкодження та витоку інформації. Вона включає широкий спектр заходів від керування паролями та захисту персональних пристроїв до забезпечення безпеки корпоративних мереж та державних систем, а головною її метою є збереження конфіденційності, цілісності та доступності інформації.

Кібербезпека захищає конфіденційні бізнес-дані, інтелектуальну власність та репутацію компаній від збитків та перебоїв в роботі. Також вона забезпечує сталий розвиток суспільства та цифрових комунікацій шляхом своєчасного виявлення та нейтралізації загроз.

В свою чергу, кіберзлочинність – це злочинна діяльність, що здійснюється за допомогою комп'ютерних систем, мереж та інформаційних технологій, яка несе безпосередню загрозу інформаційним даним та системам, державній інфраструктурі.

В українському законодавстві ці діяння є злочинними і регулюються відповідними статтями Розділу XVI Кримінального кодексу України (далі – КК України) (злочини у сфері використання електроннообчислювальних машин), зокрема, статтями 361 (несанкціоноване втручання в роботу комп'ютерних систем), 361-1 (створення та розповсюдження вірусів); 361-2 (несанкціоновані дії з інформацією), 362 (несанкціоновані дії з інформацією, яка обробляється в ЄОМ).

Отже, кіберзлочинність – це будь-які дії навмисного характеру, що пов'язані з використанням комп'ютерів, комп'ютерних мереж або інших цифрових пристроїв для скоїння дій, що кваліфікуються КК України як злочини.

До кіберзлочинності можна віднести:

- а) фішинг – викрадення особистих даних через підроблені веб-сайти або електронні листи;
- б) онлайн-шахрайство з використанням фальшивих інтернет-магазинів, аукціонів або телекомунікаційних засобів;
- в) встановлення шкідливого (вірусного) програмного забезпечення;
- г) соціальна інженерія (соціологічний термін), що проявляється у маніпулюванні людьми (групою людей) з метою отримання вільного доступу до їхніх особистих даних;
- д) піратство (викрадення) – незаконне розповсюдження інтелектуальної власності;

ж) кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу). Так звані «трояни», «боти»;

з) протиправний контент – пропаганда екстремізму, тероризму, наркоманії, порнографії, культу жорстокості та насильства;

і) рефайлінг – незаконна підміна телефонного трафіку;

к) мальваре – створення та послідовне розповсюдження вірусів і шкідливого програмного забезпечення;

л) кард-шерінг – надання незаконного доступу до перегляду супутникового та кабельного ТВ.

Тобто, об'єктом кіберзлочинів може стати будь-який користувач інтернету.

Слід відзначити, що ефективної системи профілактики даному виду злочинності у світі не існує через те, що шахраї – злочинці постійно вигадують все нові способи вчинення кіберзлочинів.

Але, існують деякі поради як підвищити безпеку, в тому числі й особисту, і уникнути ролі «жертви» кіберзлочинів. Серед таких заходів можна виділити (порекомендувати користувачам мережі інтернету):

а) використання захищених мереж;

б) створення надійних паролей з періодичною їх зміною;

в) використання інструментів конфіденційності та безпеки Google чи інших браузерів;

г) постійна перевірка своїх облікових записів;

д) встановлення та періодичне оновлення антивірусних програм для захисту пристроїв;

ж) бути в курсі та володіти інформацією про більш поширені способи, які використовують злочинці для того щоб розпізнавати їх.

Враховуючи сучасні виклики та необхідність покращення стану боротьби з кіберзлочинністю Уряд України в березні 2016 року прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки.

У тому ж 2016 році (червень) спочатку Президент України підписав Указ про створення Національного координаційного центру кібербезпеки, першочерговим завданням якого є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки в Україні. А у вересні того ж року, Верховна Рада України у першому читанні прийняла закон «Про основні заходи забезпечення кібербезпеки України». [1]

05 жовтня 2017 року Верховною Радою України цей закон був ухвалений в цілому. В ньому визначено основні засади функціонування національної системи кібербезпеки, а також закріплені права та обов'язки суб'єктів (держспецз'язок, міністерства, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти господарювання, якими є підприємства, установи та організації, що належать до критичної інфраструктури або надають послуги в інформаційній сфері та мають забезпечувати захист своїх інформаційних систем), що забезпечують кіберзахист. Також визначено й об'єкти кібербезпеки. [2]

Закон спрямований на захист суверенітету, територіальної цілісності України та забезпечення безпеки в кіберпросторі.

Кабінетом Міністрів України 07 березня 2025 року видано Розпорядження про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України. [3]

Тож, протидія кіберзлочинності вимагає від держави рішучих кроків і є одним з пріоритетних напрямів внутрішньої політики.

Також необхідна взаємодія з міжнародною спільнотою в боротьбі з цим відносно новим видом злочинності, який є міжнародною проблемою і не обмежується кордонами окремої країни. І тут справа не тільки правоохоронних органів, а й суспільства загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Указ Президента України Про Національний координаційний центр кібербезпеки від 07.06.2016 № 242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#Text> (дата звернення 07.10.2025).
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 07.10.2025).
3. Розпорядження Кабінету Міністрів України від 7 березня 2025 р. № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text> (дата звернення 07.10.2025).

Подільчак О.М. к.ю.н., доц.,
доцент кафедри правового забезпечення безпеки бізнесу,
Державний торговельно-економічний університет,
м. Київ

ЩОДО ЕФЕКТИВНОСТІ РОБОТИ АНТИКОРУПЦІЙНИХ ОРГАНІВ ЗА І ПІВРІЧЧЯ 2025 РОКУ

Корупція в Україні залишається однією з головних загроз національній безпеці та демократичному розвитку, відтак формування антикорупційної інфраструктури є незамінним елементом посилення міцності державних інституцій, виконання міжнародних зобов'язань України та руху до європейської інтеграції.

Відповіддю на ці виклики протягом останнього десятиліття стало створення комплексу спеціалізованих антикорупційних органів. Оцінка ефективності їх діяльності є важливим завданням для визначення шляхів удосконалення подальшої антикорупційної політики держави.

До системи антикорупційних органів України відносяться: Національне антикорупційне бюро України (НАБУ), що здійснює досудове розслідування щодо «топ»-корупції; Спеціалізована антикорупційна прокуратура (САП), що відповідає за здійснення нагляду за додержанням законів під час проведення оперативно-розшукової діяльності, досудового розслідування НАБУ, підтримання державного обвинувачення в суді у відповідних провадженнях та інше; Вищий антикорупційний суд (ВАКС) – суд, компетентний здійснювати правосуддя відповідно до визначених законом засад та процедур судочинства з метою захисту особи, суспільства та держави від корупційних і пов'язаних із ними кримінальних правопорушень та судового контролю за досудовим розслідуванням цих кримінальних правопорушень, дотриманням прав, свобод та інтересів осіб у кримінальному провадженні, а також вирішення питання про визнання необґрунтованими активів та їх стягнення в дохід держави у випадках, передбачених законом, у порядку цивільного судочинства; Національне агентство з питань запобігання корупції (НАЗК) – орган превентивного характеру, відповідальний за формування антикорупційної політики та запобігання корупції, здійснення контролю за фінансовими деклараціями, моніторинг способу життя посадових осіб та стеження за дотриманням обмежень щодо фінансування політичних партій тощо.

Безумовно, резонансні розслідування НАБУ та САП, спеціалізоване антикорупційне судочинство, відкритість електронного декларування повинні сприяти зменшенню рівня корупції у суспільстві. Але усі ці досягнення нівелюються відсутністю невідворотності покарання, «втечами» за кордон ключових фігурантів справ, розтягування справ на роки та значним навантаженням на бюджет країни.

Витрати з бюджету країни на утримання антикорупційних органів є однією зі складових «ціни злочинності». Це поняття, за визначенням кримінологів, включає в себе збитки, які заподіює злочинність, та витрати на протидію їй [1, с. 156]. Корупція завдає збитків практично в усіх сферах суспільного життя, призводить до втрат бюджету внаслідок розкрадання або неефективних витрат (наприклад, завищені ціни в держзакупівлях), скорочення інвестицій,