

6. Погорецький М. А., Гринюк В. О. Повідомлення судді про підозру: проблемні питання правового регулювання, теорії та практики. *Вісник кримінального судочинства*. 2018. № 2. С. 58–71. URL: <https://vkslaw.com.ua/index.php/journal/article/view/272/244>
7. Погорецький М. А., Старенький О. С. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України*. 2018. № 8. С. 85–106. URL: <http://jnas.nbuv.gov.ua/article/UJRN-0000976271>
8. Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.
9. Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань: Закон України від 15 трав. 2003 р. № 755-IV. URL: <https://zakon.rada.gov.ua/laws/show/755-15#Text>
10. Сергєєва Д. Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. Вип. 91. Ч. 4. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/344310>
11. Сергєєва Д. Б. Допустимість доказів в теорії та КПК 2012 року. *Вісник кримінального судочинства*. 2015. № 3. С. 80–87. URL: <https://vkslaw.com.ua/index.php/journal/article/view/708/625>
12. Сергєєва Д. Б. Судові експертизи у кримінальному провадженні : навч. посіб. Київ : Алерта, 2025. 262 с.
13. Шумило М. Є., Погорецький М. А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського інституту внутрішніх справ*. 2001. Вип. 3. С. 199–209.
14. Pogoretskyi M. A., Serhieieva D., Pogoretskyi M. M., Lysachenko Y., Denysenko G. Human rights guarantees in the activities of law enforcement agencies of Ukraine. *Amazonia Investiga*. 2023. Vol. 12, No. 64. P. 249–256. DOI: <https://doi.org/10.34069/AI/2023.64.04.24>. URL: <https://amazoniainvestiga.info/check/64/24-249-256.pdf>

Шрамко Дар'я Олександрівна,
здобувач ступеня вищої освіти бакалавра
інституту заочного та дистанційного
навчання Національної академії
внутрішніх справ
Науковий керівник:
доцент кафедри криміналістики
навчально-наукового інституту права
та психології Національної академії
внутрішніх справ, кандидат юридичних
наук, доцент **Семенов В. В.**

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У XXI сторіччі набуває швидкого розвитку інформаційно-технологічний процес. Виникають зовсім нові можливості для кожної людини, нові виклики та нові засоби, які дозволяють облегшити своє життя, заробити грошей або навпаки створюють такі умови, коли людина втрачає все що заробляла довгі роки. Відповідно до цього, кожен інформаційно-технологічний процес має бути врегульований на законодавчому рівні в кожній розвинутій країні.

Особливої уваги потребує дослідження кіберзлочинів в електронних мережах, оскільки з появою нових інформаційно-технологічних процесів,

виникають і нові можливості для скоєння кіберзлочинів, а оскільки держава не встигає створити нормативні умови захисту прав людини стосовно нових процесів, злочинець виходить «сухим із води».

Тому, з метою протидії кіберзлочинів необхідне подальше проведення досліджень соціального та криміналістичного напрямку щодо вивчення психофізіологічних властивостей кіберзлочинців, удосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері забезпечення інформаційної безпеки, поліпшення змісту вищої освіти фахівців з інформаційної безпеки держави.

Важливим досягненням України в боротьбі з кіберзлочинністю стало прийняття від 5 жовтня 2017 року Закону України «Про основні засади забезпечення кібербезпеки України». Пунктом 8 ст. 1 Закону розтлумачено поняття кіберзлочину, ним є суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Основним міжнародним договором України в цьому питанні є приєднання до Конвенції про кіберзлочинність, яка відбулась 23 листопада 2001 року та була ратифікована Україною 7 вересня 2005 року після чого набрала чинності 1 липня 2006 року. До основних правопорушень цієї Конвенції віднесено: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями; підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами; дитяча порнографія в мережі; порушення авторських та суміжних прав тощо [2].

На сьогоднішній день, в Кримінальному кодексі України (далі – КК України) закріплено покарання за скоєння наступних кіберзлочинів: шахрайство в інформаційних системах (ст. 190 КК України); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200 КК України); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України); несанкціоноване втручання в роботу інформаційних (автоматизованих) електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361² КК України); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363¹ КК України) тощо [3].

Кількість кіберзлочинів зростає та потребує аналізу їх характеристик з метою їх протидії та кращого розслідування. Доцільно виокремити наступні інноваційні підходи до розслідування цієї групи кіберзлочинів: використання штучного інтелекту та машинного навчання; запровадження цифрової

криміналістики як ключової складової у розслідування кіберзлочинів; кадрова складова у виді висококваліфікованих фахівців; публічно-приватне партнерство; уніфікація міжнародних стандартів [4, с. 72–74].

Проте перелік наявних кіберзлочинів не встигає за швидким темпом розвитку інформаційно-технічних процесів сучасності. Насамперед це пов'язане з виникненням нового електронного процесу, який дуже швидко розповсюджується мережею «Інтернет», коли на розробку, узгодження, переробку, прийняття нового законопроекту в будь-якій країні світу, в тому числі і в Україні, займає не один рік, а коли такий законопроект повноцінно стає законом, процес який він регулює набуває значного розвитку і виникає потреба в оновленні деяких положень закону.

Як приклад можна навести сучасні явища, такі як NFT процеси, кріптовалюта, STEPn, соціальні медіа (Tik-Tok, Instagram, YouTube), мережі 5G тощо. Досі існує певна неузгодженість у законодавстві та розповсюдженість правопорушень в таких сферах як онлайн-банкінг, захист від піратства, захист від плагіату, контролю штучного інтелекту тощо.

У реаліях сьогодення потрібно зазначити, що ще 03.03.2021 р. організація CERT-UA спостерігала збільшення кількості кібератак з використанням шкідливого програмного забезпечення, такого як Piterodo, хакерських угруповань підлеглих «рф». А з початку повномасштабної війни «рф» з Україною Україна зазнала більше двохста російських кібератак, що свідчить про скоєні кіберзлочини з боку «рф» направлені на державну інформаційну безпеку України [5; 6].

Підсумовуючи, як бачимо кібербезпека грає важливу роль в сучасному світі, так як у кожній країні має бути розроблена потужна система захисту державної інформації, захисту інформації кожного громадянина і кожного підприємства, що дозволить протидіяти кіберзлочинам, пом'якшувати наслідки кіберзлочинів, або взагалі їх притискати. Нажаль сьогоднішній розвиток нормативно-правових актів не співпадає з реаліями розвитку інформаційно-технологічних процесів. З кожним роком електронні процеси набувають все стрімкішого й стрімкішого розвитку, тому необхідно створити дієвий механізм прийняття законів в Україні, який дозволить хоча б з невеликим відривом йти за цим прогресом.

Отже, розслідування кіберзлочинів є складним і багатозадачним процесом, і для його виконання потрібні спеціальні навички та технічні ресурси. Успіх у боротьбі з кіберзлочинністю залежить від інновацій, таких як використання штучного інтелекту, розробка цифрової криміналістики, спеціалізоване навчання кадрів і міжнародне співробітництво.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. Дата оновлення: 15.12.2023 р. Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 403.
2. Конвенція про кіберзлочинність від 23.11.2001 р. Ратифікована Законом України № 2824-IV від 07 верес. 2005 р. Відомості Верховної Ради України (ВВР), 2006, № 5-6, ст. 71.
3. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. Дата оновлення: 01.03.2024 р. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131.
4. Ларченко М. Деякі особливості розслідування кіберзлочинів. *Науковий вісник Львівського державного університету внутрішніх справ*. 2024. № 3. С. 70–77.

5. Поновлення кібератак з використанням ШПЗ Pterodo хакерського угруповання Armageddon/Gamaredon 2021. Computer Emergency Response Team of Ukraine. URL: <https://cert.gov.ua/article/10702>.

6. З початку війни Україна зазнала майже 240 російських кібератак – Microsoft. Офіційний вебсайт «Суспільне новини». URL: <https://suspihne.media/233396-z-pocatku-vijni-ukraina-zaznala-majze-240-rosijskih-kiberatak-microsoft/>.

Щирук Микола Миколайович,
здобувач ступеня доктора філософії
Науково-дослідного інституту
публічного права

УЧАСТЬ ЗАХИСНИКА ПІД ЧАС ОБШУКУ В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ПРО ПРИВЛАСНЕННЯ, РОЗТРАТУ МАЙНА АБО ЗАВОЛОДІННЯ НИМ ШЛЯХОМ ЗЛОВЖИВАННЯ СЛУЖБОВИМ СТАНОВИЩЕМ: ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ

Обшук у кримінальних провадженнях про привласнення, розтрату майна або заволодіння ним шляхом зловживання службовим становищем належить до слідчих (розшукових) дій, під час яких найбільш виразно виявляється необхідність забезпечення належного співвідношення між потребами досудового розслідування та гарантіями прав особи. Його проведення пов'язане з істотним втручанням у сферу приватного життя, недоторканність житла чи іншого володіння, право власності, професійну таємницю та інші охоронювані законом інтереси. Саме тому участь захисника під час обшуку не може зводитися до формальної присутності при проведенні цієї слідчої (розшукової) дії, а повинна розглядатися як самостійний напрям реалізації функції захисту, що включає перевірку законності підстав обшуку, контроль за дотриманням меж судового дозволу, фіксацію процесуальних порушень, участь у роботі з вилученими речами та документами і подальше використання виявлених порушень для оцінки допустимості доказів [3; 9; 11]. Такий підхід узгоджується з вимогою забезпечення особі ефективної, реальної та практичної правничої допомоги, оскільки присутність захисника під час обшуку має набувати змістовного характеру і забезпечувати реальну можливість впливати на дотримання процесуальних гарантій та захищати права клієнта [10].

У кримінальних провадженнях зазначеної категорії значення обшуку зумовлене особливостями механізму вчинення відповідних кримінальних правопорушень. Доказова інформація нерідко міститься у фінансово-господарській документації, договорах, первинних бухгалтерських документах, електронній пошті, мобільних пристроях, комп'ютерній техніці, внутрішніх інформаційних системах підприємств, засобах доступу до банківських рахунків та державних реєстрів. За таких умов обшук може мати значний доказовий потенціал, але водночас створює підвищений ризик вилучення документів та носіїв інформації, які не мають безпосереднього зв'язку з предметом доказування. Науково обґрунтованою видається вимога про те, що межі обшуку повинні бути чітко визначені як на стадії судового контролю, так і безпосередньо під час його проведення [4; 5; 13].