

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет адвокатури та антикорупційної діяльності
Кафедра організації судових,
правоохоронних органів та адвокатури

АДВОКАТУРА: МИНУЛЕ, СУЧАСНІСТЬ ТА МАЙБУТНЄ

**МАТЕРІАЛИ
XV Міжнародної
науково-практичної конференції**

*14 листопада 2025 року,
м. Одеса*



Одеса
«Юридична література»
2025

УДК 347.965(477)(063)
A288

Редакційна колегія:

Н. М. Бакаянова (голова), завідувачка кафедри організації судових,
правоохоронних органів та адвокатури;
С. К. Костенко, професор;
І. О. Кісліцина, доцент;
М. О. Кравченко, доцент;
О. Г. Свида, доцент;
П. М. Синицин, доцент;
О. О. Храпенко, доцент;
Л. П. Нестерчук, старший викладач;
Р. Р. Щербатий, асистент

Рекомендовано до друку вченою радою Національного університету «Одеська юридична академія» (протокол № 3 від 15 жовтня 2025 р.)

Адвокатура: минуле, сучасність та майбутнє : матеріали XV Міжнародної науково-практичної конференції (м. Одеса, 14 листопада 2025 р.) / редкол.: Н. М. Бакаянова (гол.), І. О. Кісліцина, М. О. Кравченко [та ін.]. — Одеса : Юридична література, 2025. — 664 с.

ISBN 978—966—419—456—0

У збірнику містяться матеріали доповідей XV Міжнародної науково-практичної конференції «Адвокатура: минуле, сучасність та майбутнє», яка відбулася 14 листопада 2025 р. у Національному університеті «Одеська юридична академія». Доповіді учасників присвячені актуальним питанням адвокатури і здійснення адвокатської діяльності в Україні, історії адвокатури, діяльності Національної асоціації адвокатів України, проблемам і перспективам розвитку адвокатського самоврядування, правилам адвокатської етики та юридичній відповідальності адвокатів, зарубіжному і міжнародному досвіду організації та діяльності адвокатури.

УДК 347.965(477)(063)

Відповідальність за зміст та достовірність поданого матеріалу несуть учасники конференції, їхні наукові керівники та рецензенти, які рекомендували ці матеріали до друку.

ISBN 978—966—419—456—0

© Національний університет
«Одеська юридична академія», 2025

Чернова М. Я.

студентка 3-го курсу Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ ЗАХИСТУ АДВОКАТСЬКОЇ ТАЄМНИЦІ В УМОВАХ ЦИФРОВІЗАЦІЇ АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ

У сучасному світі цифровізація відіграє надзвичайно важливу роль у всіх сферах суспільного життя. За дослідженням Комарницької І. І., розвиток цифрових технологій має як позитивні (підвищення ефективності, оперативність обміну інформацією, розширення можливостей взаємодії), так і негативні наслідки. Вони створюють нові виклики для інформаційної безпеки, особливо у професійній діяльності юристів, де конфіденційність є ключовим елементом [1].

Хоча цифровізація оптимізує робочі процеси [2], вона створює нові ризики. Однією з ключових етичних і професійних обов'язків адвоката є збереження адвокатської таємниці, що ускладнюється в умовах цифровізації, оскільки більшість робочої інформації нині зберігається на електронних носіях або в хмарних сервісах. Це підвищує ризик несанкціонованого доступу, кібератак чи витоку конфіденційних даних, тому інформаційна безпека стає необхідною умовою для забезпечення належного рівня захисту адвокатської таємниці.

У сучасному світі недостатньо дотримуватись етичних норм — необхідно володіти знаннями з інформаційної безпеки, використовувати надійні технічні засоби захисту та перевірені платформи. Важливо також розуміти, які дії вжити, якщо стався витік інформації: як реагувати, повідомити компетентні органи та мінімізувати шкоду. Від підготовленості адвоката до цифрових викликів залежить його професійна репутація та довіра суспільства до інституту адвокатури.

Одним із ключових аспектів інформаційної безпеки є захист електронних даних та кореспонденції. Практика ЄСПЛ демонструє, що навіть законні дії правоохоронних органів можуть порушувати адвокатську таємницю без належних гарантій. У справі *Robathin v. Austria* (2012) ЄСПЛ встановив порушення статті 8 Конвенції, оскільки «вилучення та перевірка всіх даних виходила за межі того, що було необхідним» [3]. Суд підтвердив, що адвокатська таємниця охоплює й електронні носії. У справі *Sijrvulo & Associados — Sociedade de Advogados, RL v. Portugal* (2015) суд також аналізував достатність механізмів захисту при вилученні електронних листів, що демонструє потребу цифрових каналів у процедурних гарантіях і вказує на те, що інформаційна безпека є не лише технічною, а й правовою кате-

горією. Необхідний багаторівневий захист: шифрування, обмежений доступ та наявність процедур контролю.

У цифрову епоху захист адвокатської таємниці ускладнюється новими ризиками. І. Гордусь наголошує на таких загрозах, як кібератаки, фішинг, соціальна інженерія та витік даних [4]. Адвокатська таємниця (ст. 22 Закону України «Про адвокатуру та адвокатську діяльність») охоплює будь-які відомості про клієнта [5]. У цифрову епоху її захист передбачає дотримання стандартів: двофакторна автентифікація, шифрування даних та використання месенджерів із наскрізним шифруванням (Signal, Threema). Обов'язковим є захист робочих пристроїв та офісної мережі. Реагування на інциденти кібербезпеки передбачає негайне відключення пристроїв, фіксацію події, повідомлення клієнта та звернення до кіберполіції [6].

Цифрові ризики для адвокатської таємниці обумовлені низкою загроз, зокрема людським фактором (60 % витоків), фішингом та метаданими документів (DOCX, PDF), які можуть розкривати конфіденційну інформацію. Основні правила комунікації вимагають уникнення незахищених каналів. Для електронної пошти рекомендовано сервіси з наскрізним шифруванням (ProtonMail) замість публічних (Gmail). Документи слід шифрувати (VeraCrypt), а для передачі файлів використовувати безпечні інструменти (OnionShare). Хмарні сховища повинні підтримувати технологію «zero-knowledge» (ProtonDrive). Рекомендованими є месенджери Signal та Threema, тоді як WhatsApp, Telegram та Viber слід використовувати з обережністю. Соціальні мережі також становлять ризик витоку. Офісна безпека (WPA3, політика паролів), план реагування на злам та принцип резервування 3–2–1 є критично важливими.

Цифрова гігієна передбачає регулярні оновлення, сканування пристроїв (Exodus Privacy, MVT, антивіруси) та мінімізацію цифрового сліду [4]. Розширені заходи захисту поглиблюють ці принципи, починаючи з розробки чітких внутрішніх політик безпеки та протоколів поведінки з даними, підкріплених регулярними тренінгами. На технічному рівні це означає посилення мережевої інфраструктури через сегментацію (VLAN) та системи виявлення вторгнень (IDS/IPS). Критично важливим є управління доступом за «принципом найменших привілеїв», щоб обмежити доступ співробітників лише до необхідної інформації. Адвокат також має активно очищувати метадані з документів (наприклад, через Mat2), використовувати віртуальні машини для ізоляції неперевіраних файлів та покладатися на хмарні сервіси з шифруванням «zero-knowledge». Належна фізична безпека офісу, деталізований план реагування на кіберінциденти та політика безпечного архівування й видалення даних завершують комплексний захист.

Наслідки ігнорування цифрової гігієни можуть бути катастрофічними: втрата довіри, судові позови та дисциплінарна відповідальність. За даними IBM Security 2023, середня вартість витоку даних становить \$4,45 млн; у юридичній сфері це підтвердив кейс Grubman Shire Meiselas & Sacks (2020), де було викрадено 756 ГБ даних [7]. В українському контексті (ЄСІКС, Дія.Підпис) дотримання цих правил є вимогою Закону України «Про захист персональних даних» та GDPR [7].

Дослідження ролі інформаційної безпеки в умовах цифровізації адвокатської діяльності демонструє її фундаментальну трансформацію: з допоміжної технічної функції вона перетворилася на ключовий механізм забезпечення професійного обов'язку адвоката — збереження адвокатської таємниці. Цифровізація, оптимізуючи роботу, створює критичні вразливості (фішинг, соціальна інженерія, витік метаданих), що підтверджується практикою ЄСПЛ (*Robathin v. Austria*) та звітами про вартість витоків (IBM, кейс Grubman). Ефективний захист вимагає від адвокатів переходу до проактивної «цифрової гігієни» та свідомої відмови від вразливих інструментів на користь спеціалізованих рішень: E2EE-комунікаторів (Signal, Threema), шифрування дисків (VeraCrypt) та «zero-knowledge» хмарних сервісів (ProtonDrive).

Таким чином, інформаційна безпека сьогодні є невід'ємною складовою професійної компетенції адвоката, стаючи запорукою довіри клієнта, захисту репутації та збереження самої суті інституту адвокатури в цифровому світі.

Список використаної літератури

1. Комарницька І. І. Цифровізація та інформаційні технології у професійній діяльності адвоката в сучасних умовах. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. С. 243–247. URL: <http://journal-app.uzhnu.edu.ua/article/view/316974/307479>
2. Филиппук О. В. Цифровізація адвокатської діяльності: адміністративно-правовий аспект. *Правова доктрина, правотворення та правозастосування: проблеми зв'язку та шляхи розвитку*. Харків, 2024. С. 207–211.
3. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 1950. Council of Europe. URL: https://www.echr.coe.int/documents/convention_eng.pdf
4. Гордусь І. Основи цифрової безпеки для адвокатів. *Офіційний вебсайт Вищої школи адвокатури НААУ*. 2023. URL: <https://www.hsa.org.ua/lectors/gordus-igor/articles/osnovi-cifrovoyi-bezpeki-dlia-advokativ>
5. Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 № 5076-VI. URL: <https://zakon.rada.gov.ua/laws/show/5076-17#Text>
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

7. Філімонов М., Рабко Т. Юридична практика та інформаційна безпека. Київ: Вища школа адвокатури. 2025. URL: <https://tinyurl.com/59azp2n3>

Науковий керівник: кандидат юридичних наук, доцент кафедри юстиції Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка *Кухнюк Дмитро Володимирович*

Шарко С. В.

студентка 2-го курсу факультету
прокуратури та слідства (кримінальної юстиції)
Національного університету «Одеська юридична академія»

АДВОКАТСЬКА ТАЄМНИЦЯ: СУЧАСНІ ВИКЛИКИ В УМОВАХ ВОЄННОГО СТАНУ

В умовах воєнного стану особливої актуальності набуває питання захисту прав та інтересів громадян, адже основним завданням адвокатури є забезпечення охорони встановлених законом прав, свобод та інтересів людини в усіх сферах її життєдіяльності.

Відповідно до статті 59 Конституції України, кожен має право на професійну правничу допомогу. У випадках, передбачених законом, ця допомога надається безоплатно. Кожен є вільним у виборі захисника своїх прав [1]. У статті 131–2 Основного Закону зазначається, що для надання професійної правничої допомоги в Україні діє адвокатура. Незалежність адвокатури гарантується. Засади організації і діяльності адвокатури та здійснення адвокатської діяльності в Україні визначаються законом. Виключно адвокат здійснює представництво іншої особи в суді, а також захист від кримінального обвинувачення [1].

Законом України «Про адвокатуру та адвокатську діяльність» (далі — Закон) визначено, що професійні права, честь і гідність адвоката гарантуються та охороняються Конституцією України, цим Законом і іншими нормативно-правовими актами. Зокрема, пунктом 2 частини першої статті 23 Закону передбачено заборону вимагати від адвоката, його помічника, стажиста, працівників адвокатського бюро чи об'єднання, а також осіб, у яких припинено або зупинено право на заняття адвокатською діяльністю, розкриття відомостей, що становлять адвокатську таємницю [2]. Відповідно до статті 22 Закону, адвокатською таємницею є будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надан-