# ODDÍL 11. PRÁVO

Вільчик Т.Б.

## *§11.1 АДВОКАТСЬКА ДІЯЛЬНІСТЬ В УМОВАХ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ*

**Вступ.** Цифрові інформаційні технології стали глобальною тенденцією світового розвитку. Сучасні технологічно розвинуті країни вже багато років крок за кроком проводять цифровізацію, яка спрямована на створення єдиного цифрового ринку, загального простору цифрової довіри, широкого запровадження технологій із використанням штучного інтелекту. Інформаційні технології стрімко входять й у сферу діяльності адвокатури. З їх розвитком усе більша кількість документів та іншої інформації зберігається в електронному вигляді, усе більше комунікацій здійснюються адвокатом за допомогою сучасних технологій, використання яких не тільки дає нові професійні можливості, але і породжує нові загрози порушення професійної таємниці адвоката. Відомості, що становлять адвокатську таємницю, часто можуть передаватися в незашифрованому вигляді і, як результат, випадково або навмисно стати доступними третім особам. При цьому найчастіше і адвокат, і клієнт є звичайними користувачами комп'ютеру і не володіють достатніми спеціальними знаннями у сфері захисту інформації та захисту персональних даних, що дали б змогу застосувати певні засоби та методики захисту. Сьогодні поняття інформаційного забезпечення адвокатської діяльності законодавством України не лише не врегульоване, але й не відповідає у цієї частині сучасним вимогам. Наразі відсутня будь-яка офіційна консолідована інформація щодо кількості он-лайн сервісів та інтернет-ресурсів, які використовує або

адмініструє Національна асоціація адвокатів України, [1 , с. 7] що у свою сергу, вимагає активізації зусиль у сфері цифровізації адвокатської діяльності, розробці не тільки конкретних рекомендацій для адвокатів у цієї нової та важливої галузі їх роботи, але й запровадження діяльності у таких важливих напрямках, як: забезпечення цифрових сервісів для адвокатів; розробка і впровадження біометричного адвокатського посвідчення. ідентифікація автора запитів адвокатів; інформатизація діяльності органів адвокатського самоврядування, тощо [2, с.225], у тому числі, і з врахуванні досвіду зарубіжних країн.

**Виклад основного матеріалу.** З 15 грудня 2021 року починає діяти Інформаційно-телекомунікаційна система досудового розслідування, (далі -ІТСДР), проголошується рівність правового статусу паперових та електронних документів. Захисник та інші учасники кримінального провадження можуть використовувати систему під час реалізації своїх повноважень (ст. 106-1 КПК України) [3]. Кінцевою метою впровадження ІТСДР є мінімізація та, як наслідок, повна відмова в майбутньому від паперового провадження на всіх стадіях досудового розслідування та розгляду справи в суді. 17 серпня 2021 року Вища рада правосуддя затвердила Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи № 1845/0/15-21 [4], відповідно до якого процесуальні документи та докази можуть подаватися до суду в електронній формі, а процесуальні дії – вчинятися в електронній формі виключно за допомогою ЄСІТС з використанням власного кваліфікованого електронного підпису, прирівняного до власноручного підпису. На сьогоднішній день модуль «Електронний суд» не

працює для кримінального судочинства в тому режимі, як при розгляді цивільних, господарських і адміністративних справ. Як зазначила член Вищої ради правосуддя Л. Шевцова, для того, щоб можливо було розглядати в електронному вигляді кримінальні справи, повинен бути отриманий експертний висновок стосовно захищеності цієї інформації в мережі інтернет. За її словами, такого експертного висновку наразі у нас немає [5].

Інформаційну безпеку адвокатській діяльності визначають як «захист інформації конфіденційного характеру в її цілісному, тобто неспотвореному вигляді, а також інформації, яка знаходиться в режимі таємниці, необхідної для здійснення адвокатської діяльності» [6, с.425]; як «стан захищеності інформації, що становить предмет адвокатської таємниці, при якому забезпечуються її конфіденційність, цілісність і доступність» [7]; як «комплекс правових норм і відповідних їм інститутів безпеки, які гарантують надійний стан захищеності життєво важливих інтересів адвоката, клієнта, суспільства і держави…» [8,с.46]. Інформацію, яка підлягає безпеці, поділяють на таку, що належить юристу (безпека особистої інформації юриста), а також на інформацію, яка підлягає конфіденційності у взаєминах юрист-клієнт [9, с. 159]. В зв'язку з чим доречно визначати необхідність забезпечення безпеки не тільки інформації, що містить адвокатську таємницю, але й безпеки самого адвоката [8,с.47], тобто інформаційну безпеку відомостей, що складають його особисту інформацію.

Інформаційна безпека адвокатської діяльності має специфічний характер внаслідок особливості самої професії, головним принципом якої є конфіденційність. Тісний зв'язок понять інформаційної безпеки адвокатської діяльності та адвокатської таємниці вже досліджувався науковцями, і ними

були зроблені висновки про те, що, по-перше, поняття інформаційної безпеки адвокатської діяльності включає в себе поняття адвокатської таємниці, тобто є більш широким, а по-друге, що, виходячи з системного тлумачення Закону України «Про адвокатуру та адвокатську діяльність» та Правил адвокатської етики, адвокат зобов'язаний не тільки зберігати адвокатську таємницю, але і забезпечувати інформаційну безпеку в своїй професійній діяльності [8; 10, с.35]. Адвокатська таємниця «є специфічною ознакою, характерною рисою адвокатської діяльності. Це те, без чого адвокатська діяльність трансформується в суто консультаційну роботу, є тією суттєвою ознакою, без якої і саме явище втрачає свою суть, свою змістовну характеристику» [11 с.3]. К сучасним загрозам інформаційної безпеки адвокатської діяльності та, відповідно, адвокатської таємниці, можна віднести втрати або розкрадання, доступ інших осіб до цифрових носіїв інформації, що містять інформацію по справах клієнтів (ноутбуки і планшети, телефони), а також комп'ютерні зломи, кіберзлочини. Так, застосовуються різні варіанти шахрайства з використанням особами, зацікавленими в дискредитації адвоката, його вигаданих сторінок і розміщенням інформації від імені адвоката; поширення шкідливих програм, які, проникаючи в комп'ютер, роблять недоступною для користувача важливу інформацію, що міститься в ньому, з метою подальшого вимагання грошових коштів за відновлення доступу до неї; поширення неправдивих відомостей про адвоката, які посягають на його честь та гідність та можуть суттєво вплинути на вибір адвоката потенційним клієнтом [12,с.55]. Фішинг - це кіберзлочин, при якому хакер видає себе за законну установу або особу, щоб «заманити» кого-небудь для надання конфіденційної інформації, такої як паролі, дані

банківського рахунку, тощо [13]. Хакери також можуть видавати себе за законного відправника, щоб спокусити одержувача відкрити файл або веб-посилання, яка викликає завантаження шкідливого ПО на комп'ютер (також відома як «шкідливе посилання») [14]. Уявляється доцільним інформування органами адвокатського самоврядування адвокатів про нові способи комп'ютерних злочинів на постійній основі. Це дозволило б адвокату попередити можливий наступ таких злочинів [15,с.197].

При збереженні інформації на цифрових джерелах, хмарних ресурсах носії таємниці зобов'язані забезпечити її безпеку шляхом використання паролів, шифрів, криптографічних програм. Крім того, при використанні віртуальних («хмарних») серверів адвокат повинен враховувати наступні особливості зберігання інформації на них: 1) визначити юрисдикцію власника таких серверів та переконатися, що закони країни фактичного місцезнаходження сервера встановлюють високі стандарти конфіденційності; 2) ліквідація підприємства-власника серверів неминуче призведе до втрати інформації, яка є конфіденційною юридичної інформацією; 3) провайдер (технологічний посередник для надання доступу до мережі Інтернет), і, отже, суб'єкт, який отримав в системі безпеки провайдера, має негайний доступ до інформації в момент її передачі з пристрою адвоката на віртуальний сервер [16,с. 7].

На окрему увагу заслуговують месенджери (Skype, ICQ, Viber, WhatsApp, Telegram, Line, Facebook Messenger), які отримали популярність серед адвокатів завдяки здатності передавати не тільки текст, голосові і відеоповідомлення, а й файли. Незважаючи на те, що кожен з цих месенджерів має певні особливості щодо захисту інформації та положення про

конфіденційність, вони не одноразово піддавалися атакам хакерів, в результаті чого відбувався витік інформації. Також не варто забувати і про можливості цілеспрямованого зняття інформації з каналів зв'язку. Крім того, на практиці нерідкі випадки, коли адвокати за попереднім погодженням з клієнтами навмисне передають інформацію в ЗМІ, що є частиною обраної стратегії захисту прав та інтересів клієнта і передбачає контрольований витік інформації, яка містить адвокатську таємницю, що допустимо в інтересах клієнта [17].

Адвокатське досьє є одним із способів збереження таємниці клієнта та забезпечення конфіденційності інформації. Питання ведення адвокатського досьє регулюється Положенням, затвердженим Рішенням Ради адвокатів України №169 (2017), у якому зазначено, що досьє адвоката - сукупність документів та інформації, що отримуються, збираються, створюються, зберігаються, використовуються адвокатом (іншою особою за його дорученням) та/або знаходяться в його розпорядженні (володіння, віданні тощо) і охоплюється поняттям адвокатської таємниці, а також окремі (одиничні) документи та будь-які носії інформації, які охоплюються таким поняттям, предмети, тощо. Досьє адвоката може зберігатися повністю або частково в електронній формі [18]. Аналіз тексту Положення приводить до висновку щодо відсутності у ньому конкретних рекомендацій, спрямованих на забезпечення інформаційної безпеки адвоката або «техніки безпеки адвоката», як вказано у Положенні. Так, розділ IV. Положення під назвою «Конфіденційність» містить усього два пункти, які дублюють зміст певних частин статті 22 Закону України «Про адвокатуру та адвокатську діяльність», присвяченій адвокатській таємниці. Враховуючи те, що адвокатське досьє є одним із способів збереження адвокатської

таємниці, відомості і матеріали, що містяться в ньому, не можуть бути використані як докази обвинувачення. Отже, ведення адвокатського досьє дозволяє адвокату забезпечити безпеку інформації, що становить предмет адвокатської таємниці. Адвокатське досьє не має строку зберігання і може бути знищене адвокатом з дотриманням прав та інтересів клієнта (п.1.10). Вважаємо, що вказане положення потребує своєї конкретизації. Зокрема, воно повинно передбачати конкретні терміни, порядок зберігання і утилізації даного документа, що містить адвокатську таємницю, які повинні корелюватися саме з необхідністю забезпечення останньої. Слід також доповнити вказаний документ положенням, відповідно до якого при збереженні інформації на цифрових джерелах, хмарних ресурсах носії таємниці зобов'язані забезпечити її безпеку шляхом використання паролів, шифрів, криптографічних програм.

Відсутність у адвокатів навичок комунікації за допомогою цифрових інструментів може призвести до зниження ефективності встановлення довірчих відносин з клієнтом, втрати «людяності» спілкування і, як наслідок, до помилок в прогнозі розвитку професійної комунікації, зниження ефективності професійної взаємодії. Як вражають психологи, у цифровій комунікації довірителю простіше спотворювати інформацію, а адвокату складніше верифікувати повідомлення клієнта [19]. Тому вказані відносини адвоката з клієнтом, з одного боку, спрощують багато процесів, а з іншого - вимагають підвищеної уваги і вироблення конкретних способів оптимізації взаємодії. Вважаємо, що адвокату слід до укладення договору про надання правової допомоги обговорити з клієнтом необхідні заходи щодо забезпечення цифрової безпеки інформації, яку він буду довіряти адвокату, а

також прийняти спільне рішення з даного питання, яке було б зрозумілим та влаштовувало обидві сторони. Бажано таку угоду скласти в листі-зобов'язанні або іншому письмовому вигляді про характер комунікацій та заходи безпеки цифрової інформації, які будуть (або не будуть) застосовуватися, і вказати конкретні заходи, які будуть використовуватися, наприклад, шифрування та інші конкретні заходи безпеки [20].

Так, Типові правила професійної поведінки Американської асоціація юристів (ABA) [21] передбачають, що адвокату потрібно отримати згоду клієнта й перед тим, як використовувати у своїй діяльності штучний інтелект (далі - ШІ) і така згода повинна базуватися на повному інформуванні клієнта. Повне інформування повинно містити інформацію про ризики та обмеження системи ШІ. У певних випадках рішення адвоката не використовувати ШІ також може бути обов'зковим для поінформування клієнта, якщо використання ШІ може бути корисним для нього. Вважається, що вищевказані положення можуть бути корисними і для нормативного визначення у національних актах органів адвокатського самоврядування, у тому числі – Правилах адвокатської етики.

Відповідно до Типового правила 1.6 ABA, адвокати зобов'язані дотримуватися конфіденційності щодо своїх клієнтів. Цей обов'язок вимагає, щоб адвокат «докладав розумних зусиль щодо запобігання ненавмисному або несанкціонованому розкриттю або несанкціонованому доступу до інформації, що відноситься до клієнта». Ця вимога поширюється на два аспекти - ненавмисне розкриття інформації і несанкціонований доступ. Ненавмисне розкриття інформації включає в себе такі загрози, як залишення портфеля, ноутбука або смартфона в таксі чи ресторані,

відправка конфіденційного електронного листа не тому одержувачу, розкриття конфіденційних документів або цифрових даних. Несанкціонований доступ включає такі загрози, як діяльність хакерів, злочинців, шкідливе ПЗ і внутрішні загрози. Основними факторами для визначення ступеню добросовісності адвокатів, на думку Американської асоціації юристів, слугують: цінність та значимість самої інформації; ступінь ймовірності розкриття інформації у разі невикористання додаткових заходів для її захисту, вартість використання таких додаткових заходів; складність реалізації додаткових гарантій конфіденційності; ступінь, у який вказані гарантії негативно впливають на здатність адвоката надавати кваліфіковану юридичну допомогу. Але при використанні деяких інструментів штучного інтелекту (ШІ), так як і при використанні цифрових даних, може виникнути необхідність передачі конфіденційної інформації щодо клієнта стороннім особам – провайдерам, постачальникам послуг ШІ. У такому разі адвокатам потрібно забезпечити належний захист інформації: отримати гарантії конфіденційності від сторонніх постачальників, а також відповіді на питання: як буде зберігатися інформація, які міри безпеки існують у зберіганні інформації. Офіційний висновок Постійного комітету ABA з етики та професійної відповідальності «Обов'язки юристів після злому електронних даних або кібератаки» (від 17 жовтня 2018 г.) ясно дає зрозуміти, що «вірогідність етичного порушення виникає, коли юрист не робить розумних зусиль, щоб уникнути втрати даних або виявити кібервторгнення, і що відсутність таких розумних зусиль є причиною порушення» [22].

У США та країнах Європейського Союзу на цей час склалася практика, відповідно до якої для того, щоб отримати доступ до персональних даних, які можуть бути визнані

доказами по кримінальній справі, більше недостатньо конфіскувати пристрої користувача (тобто настільні комп'ютери, ноутбуки або мобільні телефони). Найбільш релевантні дані для кримінальних розслідувань, такі як електронна пошта, фотографії або документи, тепер, як правило, зберігаються в центрі обробки даних, яким керує постачальник хмарних послуг. Утім, існують певні правові інструменти, які дозволяють правоохоронним органам в Європейському Союзі та в Сполучених Штатах домагатися розкриття хмарних даних. З огляду на те, що доступ до хмари може бути доступний з будь-якого пристрою, який має підключення до Інтернету, незалежно від його фізичного розташування, цілком імовірно, що дані користувача зберігаються за кордоном. На думку науковців, колізії законів можуть стати звичайним явищем, наприклад, коли розкриття хмарних даних одночасно передбачено законами однієї держави і заборонено законами іншої держави [23]. В різних юридичних сферах, включаючи особисту конфіденційність, інтелектуальну власність та антимонопольне законодавство,- відмічає Andrews Damon C., постійно виникають суперечки, пов'язані з хмарними даними. Перш ніж суди зможуть протистояти таким питанням, вони повинні вирішити два основних процедурних питання : по-перше, чи застосовується будь-який закон у хмарі, і якщо так, то який закон повинен застосовуватися [24]. На ці та інші запитання необхідно буде найближчим часом відповісти і національному законодавцію.

Важливою є розробка єдиних рекомендацій по роботі адвоката з електронними пристроями, підготовлених на підставі аналізу практичної адвокатської діяльності, а також взаємодії з технічними фахівцями в сфері цифрових технологій. Саме такий підхід дозволить сформувати

сукупність керівних принципів, правил, процедур і практичних прийомів в галузі забезпечення безпеки інформації, якими адвокати зможуть керуватися в ході своєї діяльності. Вважаємо, що Комітету з питань електронного судочинства та кібербезпеки адвокатської діяльності, створеному у 2019 році при НААУ, особливу увагу слід приділити розробці правил використання мобільних пристроїв при спілкуванні адвоката з довірителем (мобільних телефонів, планшетів, ноутбуків), дотримання яких дозволить забезпечити конфіденційну інформацію в епоху цифровізації. До таких заходів, зокрема можна віднести: 1) забезпечення розумної захисту від втрати мобільного пристрою. 2) використання паролів на мобільних та інших електронних пристроях, що застосовуються адвокатами, в тому числі особистих. Наприклад, установка автоматичного блокування будь-якого електронного пристрою протягом певного проміжку часу його невикористання; 3) зберігання отриманої від довірителя інформації на сервері в зашифрованому вигляді; своєчасне видалення такої інформації з особистих або недостатньо захищених пристроїв; 4) обмін (отримання і відправка) інформації з довірителем через мережу Інтернет за загальним правилом тільки в зашифрованому вигляді, особливо при використанні електронної пошти [25,с.221]. Деякі автори пропонують маркувати електронні пристрої, щоб в разі втрати їх можна було повернути власнику [26].

Адвокати зобов'язаний створити умови і вжити всіх можливих заходів для максимального захисту будь-якої інформації, отриманої і переданої їм через мережу «Інтернет», для чого їм доцільно здійснювати співробітництво з відповідними фахівцями в галузі комп'ютерних технологій. Процес цифровізації адвокатської діяльності повинен

відбуватися організовано, враховуючи різницю в цифровій компетентності серед представників різних вікових груп, рівня їх освіти, що стосується як самих адвокатів, так і їх потенційних довірителів [27].

**Висновки.** Діяльність адвоката з інформацією неможлива без забезпечення безпеки цієї інформації. Виходячи з системного тлумачення Закону України «Про адвокатуру та адвокатську діяльність» та Правил адвокатської етики, адвокат зобов'язаний не тільки зберігати адвокатську таємницю, але і забезпечувати інформаційну безпеку в своїй професійній діяльності. Поняття інформаційної безпеки адвокатської діяльності включає в себе поняття адвокатської таємниці, тобто є більш широким.

Процес цифровізації адвокатури повинен бути організованим та передбачати наявність програми розвитку цифрової компетентності адвокатів, що враховує різні рівні наявної у адвокатів цифрової компетентності. Адвокати зобов'язаний створити умови і вжити всіх можливих заходів для максимального захисту будь-якої інформації, отриманої і переданої їм через мережу «Інтернет», для чого адвокатам доцільно здійснювати співробітництво з відповідними фахівцями в галузі комп'ютерних технологій.

При використанні віртуальних («хмарних») серверів адвокати повинні враховувати певні особливості зберігання інформації на них, зокрема: отримати гарантії конфіденційності від сторонніх постачальників, а також відповіді на питання: як буде зберігатися інформація, які заходи безпеки існують у зберіганні інформації.

У Положенні, що регулює питання ведення адвокатського досьє, яке затверджено Рішенням Ради адвокатів України №169 (2017), доцільно передбачати

конкретні терміни, порядок зберігання і утилізації даного документа, що містить адвокатську таємницю, які повинні корелюватися саме з необхідністю забезпечення останньої. Слід також доповнити Положення тим, що при збереженні інформації на цифрових джерелах, хмарних ресурсах носії таємниці зобов'язані забезпечити її безпеку шляхом використання паролів, шифрів, криптографічних програм.

У зарубіжних країнах адвокати мають етичні та загальні обов'язки щодо прийняття компетентних і розумних заходів для захисту інформації, що стосується клієнтів, а також часто мають договірні та нормативні обов'язки щодо захисту конфіденційної інформації. Доцільно взяти до уваги правило, відповідно до якого до укладення договору про надання правової допомоги адвокату слід обговорити з клієнтом необхідні заходи щодо забезпечення безпеки цифрової інформації, а також прийняти спільне рішення з даного питання, яке було б зрозумілим та влаштовувало обидві сторони. Вказані правила стосуються й можливості використання адвокатом у своїх професійній діяльності штучного інтелекту.

**Список використаних джерел:**

1. Звіт Національної асоціації адвокатів України за 2020 рік. URL: https://unba.org.ua/assets/uploads/news/zvity/UNBA_ANNUAL_REPORT_2020.p df

2. Пряженникова А. Цифровые технологи в практической деятельности адвоката. Образование и право № 5. 2020. С. 223-226.

3. Закон України Про внесення змін до Кримінального процесуального кодексу України щодо запровадження

інформаційно-телекомунікаційної системи досудового розслідування. URL: https://zakon.rada.gov.ua/laws/show/1498-20#Text

4. ВРП затвердила Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи. URL: https://hcj.gov.ua/news/vrp-zatverdyla-polozhennya-pro-poryadok-funkcionuvannya-okremyh-pidsystem-moduliv-yesits

5. Членкиня ВРП Лариса Швецова нагадала адвокатам, як працює Електронний суд для кримінальних справ. URL: https://sud.ua/ru/news/publication/218134-chlenkinya-vrp-larisa-shvetsova-nagadala-advokatam-yak-pratsyuye-elektronniy-sud-dlya-kriminalnikh-sprav?fbclid=IwAR1UiY9xHlCVhTRrN2DIo2Mg4Te8DvsjiWvPv_J8dmpLNVoYlePLjNzIlQ0

6. Доклад для международной научно-практической онлайн-конференции «Формирование цифровой экосистемы адвокатуры в Азербайджанской Республике, Республике Беларусь и Российской Федерации» 18 мая 2020 г. URL: https://fparf.ru/news/fpa/tsifrovizatsiya-navsegda/

7. Боричевская В.В. Информационная безопасность в адвокатской деятельности: понятие и проблемы правового обеспечения. Устойчивое развитие экономики: состояние, проблемы, перспективы: сборник трудов X международной научно-практической конференции (г. Минск, 4 апреля 2016 г.). Пинск: ПолесГУ, 2016. С. 223-225.

8. Клименко К.О., Костенко В.В. Окремі аспекти інформаційної діяльності адвоката. 46 Том 31 (70) № 5 2020. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 31 (70) № 5 2020.С.46-51.

9. Гусятников П.П., Гусятникова П.П. Информационная безопасность адвоката: основные понятия // Пробелы в российском законодательстве. 2016. № 1.

10. Viktor Zaborovskyy. INFORMATION SECURITY IN LAWYERS'PROFESSIONAL ACTIVITIES. Конституційно-правові академічні студії. Випуск 2. 2020. С.33-38.

11. Пилипенко Ю.С. Адвокатская тайна: Теория и практика реализации: автореф. дис. … д-ра юрид. наук. М., 2009. 56 С.

12. Соловьева В.И. Проблема обеспечения сохранения адвокатской тайны в условиях цифровизации. Евразийская адвокатура. № 6 (43). 2018. С.51-55.

13. What Is Phishing? PHISHING.ORG, URL: https://www.phishing.org/what-is-phishing

14. How to Recognize a Malware Email. Michigan State University. URL: https://www.egr.msu.edu/decs/security/how-recognize-malware-email

15. А.С. Советкина, А.В. Лошкарёв, Развитие цифровизации в сфере адвокатуры и адвокатской деятельности: преимущества и возможные недостатки. International Journal of Humanities and Natural Sciences, vol. 9-2 (48), 2020. С. 197.

16. Наумов В.В. Информационная безопасность адвоката в сети «Интернет». Динамиката на съвременната наука–2017: материали XIII Международна научна практична конференция. София: «Бял. ГРАД-БГ», 2017. С. 6-11.

17. Резникова Анна. Безопасность трудна. Банковское право. Випуск 6 (1050). 2018. URL: https://pravo.ua/articles/bezopasnost-trudna/

18. Питання ведення адвокатського досьє. Рішенням Ради адвокатів України №169 (2017). URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2017-08-04-r-shennya-rau-169_59d23b518e85f.pdf

19. Скабелина Л.А. Влияние цифровизации на профессиональную коммуникацию адвоката. Адвокатская практика. № 4. 2020. URL: https://msal.ru/upload/medialibrary/e1b/Skabelina-LA-Advokatskaya-praktika-2020-4.pdf

20. David G. Ries. Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties. ON NOVEMBER 14, 2019. URL: https://www.lawpracticetoday.org/article/cybersecurity-attorneys-legal-ethical/

21. Model Rule of Professional Conduct. 2019. URL: https://www.americanbar.org/groups/professional_responsibility/publications/

22. Cybersecurity. ABA. October 16, 2019. URL: https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019

23. Юнкера Сехвани, Р. (2018). Одно облако в небе и противоречивые законы на местах: Регулирование доступа правоохранительных органов к электронным доказательствам в облачных вычислениях в Европейском Союзе и Соединенных Штатах (неопубликованный тезис). Колледж Европы, Бельгия. URL: https://doi.org/10.2139/ssrn.3271580

24. Andrews, Damon C. and Newman, John M., Personal Jurisdiction and Choice of Law in the Cloud (March 3, 2013). 73 Maryland Law Review 313 (2013), Available at SSRN: https://ssrn.com/abstract=2227671 or http://dx.doi.org/10.2139/ssrn.2227671

25. Коган М.И. Обеспечение сохранения адвокатской тайны при использовании адвокатом современных технологий и электронных девайсов. Вестник университета им. О.Е. Кутафина. № 11.2020.С. 218-223.

26. Williams C. Computing and HIPAA Privacy and Computing, (2013) Perkins Coie LLP // URL: http://www.perkinscoie.com/files/upload/PL_13_01_C.A.WilliamsHIPAAarticle.pdf.

27. Доклад для международной научно-практической онлайн-конференции «Формирование цифровой экосистемы адвокатуры в Азербайджанской Республике, Республике Беларусь и Российской Федерации» 18 мая 2020 г. URL: https://fparf.ru/news/fpa/tsifrovizatsiya-navsegda/



# MODERNÍ ASPEKTY VĚDY

*v rámci publikační skupiny*
*Scientific Publishing Group*

## *Svazek XIII mezinárodní kolektivní monografie*

Česká republika
2021

*Mezinárodní Ekonomický Institut s.r.o. (Česká republika)*
*Středoevropský vzdělávací institut (Bratislava, Slovensko)*
*Národní institut pro ekonomický výzkum (Batumi, Gruzie)*
*Batumi School of Navigation (Batumi, Gruzie)*
*Regionální akademie managementu (Kazachstán)*
*Veřejná vědecká organizace „Celokrajinské shromáždění lékařů ve veřejné správě" (Kyjev, Ukrajina)*
*Nevládní organizace „Sdružení vědců Ukrajiny" (Kyjev, Ukrajina)*
*Univerzita nových technologií (Kyjev, Ukrajina)*

*v rámci publikační skupiny Publishing Group „ Vědecká perspektiva "*

# MODERNÍ ASPEKTY VĚDY

## *Svazek XIII mezinárodní kolektivní monografie*

Česká republika
2021

*International Economic Institute s.r.o. (Czech Republic)*
*Central European Education Institute (Bratislava, Slovakia)*
*National Institute for Economic Research (Batumi, Georgia)*
*Batumi Navigation Teaching University (Batumi, Georgia)*
*Regional Academy of Management (Kazakhstan)*
*Public Scientific Organization "Ukrainian Assembly of Doctors of Sciences in Public Administration" (Kyiv, Ukraine)*
*Public Organization Organization "Association of Scientists of Ukraine" (Kyiv, Ukraine)*
*University of New Technologies (Kyiv, Ukraine)*

*within the Publishing Group "Scientific Perspectives"*

# MODERN ASPECTS OF SCIENCE

## *13- th volume of the international collective monograph*

Czech Republic
2021

**Vydavatel:**

**Mezinárodní Ekonomický Institut s.r.o.**
**se sídlem V Lázních 688, Jesenice 252 42**
**IČO 03562671 Česká republika**

Zveřejněno rozhodnutím akademické rady
Mezinárodní Ekonomický Institut s.r.o. (zápis č. 1/2021 ze dne 8. listopadu 2021)

*Monografie jsou indexovány v mezinárodním vyhledávači Google Scholar*



**Tým autorů**

C91 Moderní aspekty vědy: XIII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2021. str. 548

Svazek XIII mezinárodní kolektivní monografie obsahuje publikace o: utváření a rozvoji teorie a historie veřejné správy; formování regionální správy a místní samosprávy; provádění ústavního a mezinárodního práva; finance, bankovnictví a pojišťovnictví; duševní rozvoj osobnosti; rysy lexikálních výrazových prostředků imperativní sémantiky atd.

*Materiály jsou předkládány v autorském vydání. Autoři odpovídají za obsah a pravopis materiálů.*

## ODDÍL 10. LÉKAŘSKÁ VĚDA



## ODDÍL 11. PRÁVO

Vydavatel:

Mezinárodní Ekonomický Institut s.r.o.
se sídlem V Lázních 688, Jesenice 252 42
IČO 03562671 Česká republika

# MODERNÍ ASPEKTY VĚDY

*Svazek XIII mezinárodní kolektivní monografie*

Podepsáno k tisku 10 listopad
Formát 60x90/8. Ofsetový papír a tisk
Headset Times New Roman.
Mysl. tisk. oblouk. 8.2. Náklad 100 kopií.