УДК 343.98:343.45

Резнікова Г. І.,
кандидат юридичних наук, старший викладач
Київського національного торговельно-економічного університету,
старший юрист АО «Нацина Рачук»

ІНФОРМАЦІЙНА БЕЗПЕКА АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ: КРИМІНАЛІСТИЧНИЙ ПОГЛЯД

Анотація. У статті йдеться про те, що порушення стану інформаційної безпеки адвокатської діяльності можливе внаслідок існування внутрішніх, зовнішніх і змішаних загроз. Першим класом загроз інформаційної безпеки є внутрішні загрози адвокатської діяльності, тобто незаконна діяльність інсайдерів (адвокатів, їх помічників, стажистів, осіб, які перебувають у трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також осіб, щодо яких припинено або зупинено право на заняття адвокатською діяльністю). Другий клас загроз інформаційної безпеки адвокатської діяльності становлять зовнішні загрози кіберпростору – віруси, мережеві хробаки; фітинг, вішинг; хакерські атаки тощо. Третій клас становлять змішані форми загроз, тобто поєднання зусиль зовнішніх і внутрішні порушників інформаційної безпеки.

Ключові слова: адвокатська діяльність, адвокатська таємниця, адвокатське досьє, інформаційна безпека, інформаційні ресурси, інформаційне поле, інформаційна інфраструктура.

Постановка проблеми. Інформаційна глобалізація світового співтовариства наприкінці XX – XXI ст. детермінувала виникнення проблем, пов'язаних із забезпеченням інформаційної безпеки людства. Ера інформаційних технологій (далі – ІТ), з одного боку, відкрила світу безпрецедентні цифрові можливості створювати, використовувати та по-ширювати інформацію, а з іншого, – зумовила виникнення інформаційних загроз. Це сприяло утвердженню актуальності дослідження проблем правового та організаційно-технічного забезпечення інформаційної безпеки, стану захищеності інформаційного середовища, захисту інформаційних прав і свобод особи[1], а також необхідності використання інформаційних ресурсів в інтересах особи, суспільства і держави [21].

Забезпечення інформаційної безпеки ускладняється й тим, що нині світ гостро відчуває зміну акцентів з технологій фізичного знищення супротивників, які характерні для індустріальних суспільств, на нові «гібридні» інструменти введення війн, синтетичний характер яких дозволяє поєднати фізичний та інформаційно-психологічний вплив[2]. Переосмислені й можливості використання технологій інформаційного впливу на свідомість людей (від впливу на маркетингові показники, лобіювання інтересів чи просування певних осіб, ідей, брендів тощо до розпалювання національної (релігійної) ворожнечі, поширення ідей війни, насильницької зміни конституційного ладу країн і т. ін.). Паралельно до цього, спостерігається зростання кількості та потужності кібератак, здійснюваних в інтересах окремих країн, груп та осіб[3]. Відповідно, постійне оновлення ІТ детермінує трансформування національної і транснаціональної злочинності, зміну способів вчинення злочинів, докорінне оновлення арсеналу знарядь і засобів останніх, адже обстановка вчинення більшості злочинних посягань нині значно інформатизована.

Аналіз останніх досліджень. Відповідно, перед органами державної влади і місцевого самоврядування, представниками громадського суспільства, науковою спільнотою й особливо працівниками правоохоронних органів постає актуальне завдання – *забезпечення інформаційної безпеки особи, суспільства і держави*, яке має вирішуватися не лише шляхом удосконалення механізму правового регулювання інформаційних відносин, але й розробки і впровадження дієвих механізмів запобігання та протидії злочинам у цій сфері. Йдеться про розробку в сучасну оперативно-слідчу, судову та адвокатську практику криміналістичних прийомів, методів і рекомендацій, втілених у системі криміналістичних методик розслідування злочинів, що посягають на інформаційну безпеку особи, суспільства та держави. Останні мають ґрунтуватись на окремому криміналістичному вченні, об'єктом якого виступають ІТ, відносини, які виникають з огляду на їх використання у злочинній діяльності та діяльності із досудового розслідування та судового провадження порушень, вчинених щодо інформаційної безпеки держави, суспільства та особи. В.В. Білоус зауважує, що нині в Україні бракує досліджень теоретичних засад формування і практичного застосування ІТ у криміналістиці, місце їх у науці невизначено, а рекомендації із їх використання в судово-слідчій діяльності несформовані [1, с. 166]. Втім, зарубіжна криміналістика (наприклад, США) вже давно відносить ІТ до об'єктів наукового пізнання, зокрема, вченими запропоновано виокремлювати у системі судових наук так звану **«цифрову криміналістику»** (**Digital Forensics**). За аналогією з цим, М. М. Федотов пропонує створити нову науку – **Форензику**, присвячену розкриттю злочинів, пов'язаних з комп'ютерною інформацією, методам отримання та дослідження доказів

[1] *Примітка. Світове співтовариство погодило «Пакт про електронний ненапад», що розроблявся під егідою ООН, яким встановлено правила поведінки в Інтернеті, заборону кібератак на критичну інфраструктуру в мирний час і використання ІТ терористами з метою пропаганди незаконних дій (Див.: Пакт про електронний ненапад: 20 країн домовились не вести між собою кібервійни: Depo. Світ. – URL: https://www.depo.ua/ukr/svit/ elektronniy-pakt-pro-nepapad-20-krayin-domovilis-ne-vesti-17082015072100 (дата звернення: 01.10.2017).*

[2] *Примітка. Прикладом застосування гібридних методів війни є анексія АРК та окупація Луганської і Донецької обл. РФ. Застосування спеціальних інформаційно-психологічних операцій дозволилі ворогу сугестивно впливати на українське суспільство та світ. Такі дії руйнують систему світової та регіональної безпеки. Тому система безпеки має носити випереджувальний характер, опираючись на прогнозування та запобігання цим загроз. Прикладом такої системи кібербезпеки слугує підрозділ кіберрозвідки Ізраїлю чисельністю 7 500 операторів (це 80% складу Аману) (Див.: Филатова О. Как Израилю удается бороться с терроризмом с помощью соцсетей. – URL: http://uinp.info. (дата звернення: 01.10.2017).*

[3] *Примітка. Прикладом кібератаки в Україні є атака віруса «Petya», який шифрує файли на жорсткому диску ПК, перезаписує і шифрує головний завантажувальний запис (MBR). У результаті всі файли, що зберігаються на комп'ютері, стають недоступними, а програма вимагає грошовий викуп у біткоїнах (від 300 до 800 доларів США). Від вірусу «Petya» постраждали: Італія, Ізраїль, Угорщина, Румунія, Польща, Німеччина, Велика Британія, США, Данія, Нідерланди тощо. Втім найбільше постраждалих в Україні, – 75 % уражених ПК енергетичних компаній, банків, аеропортів, АЕС та ін. (Див.: Ransom.Petya – Removal: SYMANTEC. – URL: https://www.symantec.com/security response/writeup.jsp?docid=2016-032913-4222-99&tabid=3 (дата звернення: 01.10.2017).*

у формі електронно-цифрової інформації, застосуванню технічних засобів [25, с. 8]. З цим важко погодитись, адже в системі криміналістики одним з елементів є окрема криміналістична теорія (вчення), на статус якої й має претендувати «Форензика». Окрім того, більш вдалим є найменування – «цифрова криміналістика» або «електронно-цифрова криміналістика». Розвиток цифрової криміналістики як окремого криміналістичного вчення, дослідження природи та видів інформаційних загроз, сприятиме побудові окремих криміналістичних методик розслідування злочинів, пов'язаних з порушенням стану інформаційної безпеки особи, суспільства та держави, синтезу знань із криміналістичного забезпечення розслідування цих злочинів.

Мета статті – проаналізувати розбудову системи окремих криміналістичних методик розслідування злочинів, що посягають на інформаційну безпеку особи, суспільства та держави, і спробувати розробити криміналістичну класифікацію й характеристики цих злочинів, які є підгрунтям для формування окремих методик.

Виклад основного матеріалу дослідження. Криміналістична характеристика видів (груп) злочинів є структурним компонентом окремих криміналістичних методик розслідування злочинів, для формування якої, пише В. А. Журавель, будують криміналістичну класифікацію окремого виду чи групи злочинів. Класифікація є системоутворюючою формою різних за змістом криміналістичних характеристик [6, с. 69].

В Україні кримінальне законодавство називає групу суміжних злочинів, склади яких покликані охороняти інформаційну безпеку особи, суспільства, держави. З-поміж них можна назвати такі: ст. 111, 114, 132, 145, 163, 168, 182, 209-1, 231, 232, 232-1, 328, 329, 330, 361-2, 362, 381, 387, 397, 422 Кримінального кодексу України (далі – КК України) [14]. Ці склади злочинів утворюють окрему групу злочинів, що захищають інформаційну безпеку особи, суспільства та держави, що передбачені різними розділами Особливої частини КК України, оскільки, за визначенням законодавця, мають різні родові об'єкти. В.В. Крилов пише, що підчас аналізу протиправних дій, які вчиняються щодо документованої й комп'ютерної інформації, стає зрозуміло, що законодавець як підставу для віднесення того чи іншого делікту до родового об'єкта називає головну цінність, яка охороняється, і не звертає уваги на механізми та характер вчинюваних з інформацією дій. Між тим, нерідко «слідова картина» та способи пошуку слідів злочинів, не дивлячись на остаточної кримінально-правової кваліфікації дій, будуть достатньо схожими [16, с. 154]. Кримінально-правова класифікація злочинів є орієнтиром, базою для криміналістичних класифікаційних досліджень, пояснює В.А. Журавель, бо дозволяє визначити рівні та підрівні криміналістичної класифікації злочинів [6, с. 70]. Вчені намагались об'єднати усю сукупність злочинів у галузі інформаційних відносин в «інформаційні злочини» [16, с. 164]. Втім, практичне значення для діяльності правоохоронних органів мають криміналістичні класифікації менших груп злочинів, які виокремлено за криміналістично значущими ознаками. Так, для злочинів щодо розголошення професійних таємниць є значущими такі криміналістичні ознаки: предмет злочину, спосіб учинення злочину та особа злочинця, синтез яких дозволив побудувати криміналістичну класифікацію названої групи злочинів [23, с. 20]. Зауважимо, що якщо розголошення професійних таємниць вчиняються особою під час виконання професійних, службових чи процесуальних обов'язків, то досліджувану групу можливо диференціювати за критерієм сфери здійснення діяльності. Будь-яке розголошення таємниці вчиняється у відповідній обстановці, – *порушеному стані інформаційної безпеки певної професійної діяльності*, тому ці злочини, на підставі такої ознаки, диференціюються на підгрупи. У підгрупі злочинів щодо розголошення професійних таємниць юридичної діяльності, виокремлюється такий вид, як: ***порушення встановлених гарантій діяльності захисника чи представника особи та їх професійної таємниці***. Цей *вид*, на підставі статусу особи злочинця, можливо подальше диференціювати на *підвиди*: 1) розголошення, вчинене адвокатом; 2) розголошення, вчинене помічником адвоката; 3) розголошення, вчинене стажистом адвоката; 4) розголошення, вчинене особами, які перебувають у трудових відносинах з адвокатом, адвокатським бюро чи об'єднанням (бухгалтер, секретар та ін.); 4) розголошення, вчинене особою, право на заняття адвокатською діяльністю якої припинено або зупинено. Така криміналістична класифікація злочинів щодо розголошення професійних таємниць, яка була фундаментом у створенні криміналістичної характеристики **міжродового рівня**, може сприяти справі розбудови системи окремих криміналістичних методик розслідування групи злочинів (підгрупи, видів чи підвидів), що посягають на інформаційну безпеку особи, суспільства і держави. Зосередимо увагу на такому окремому виді злочинів, як розголошення адвокатської таємниці, що входить до названої системи криміналістичних методик розслідування злочинів.

Виток інформації з обмеженим доступом, що захищається правовим режимом адвокатської таємниці, відбувається в *обстановці порушеного стану інформаційної безпеки адвокатської діяльності*. Надання якісної правничої допомоги, здійснення захисту осіб та представництво їх інтересів адвокатом, можливе за умови дотримання головного принципу адвокатської діяльності – *конфіденційності*, порушення якого може мати місце через дії *зовнішніх* (шкідливого програмного забезпечення – вірусів, троянських програм, руткітів, шпигунів; суб'єктивно вмотивованих хакерських атак; фішингу або вішингу тощо), *внутрішніх* (інсайдерів) і *змішаних інформаційних загроз*.

Основні гарантії конфіденційності адвокатської діяльності закріплені як у *національному законодавстві України* (Конституція України [11], Кримінальний кодекс України [14], Кримінальний процесуальний кодекс України [12], Закон України «Про адвокатуру та адвокатську діяльність» [25] і т. ін.), так і у **міжнародних актах** (Європейська конвенція про захист прав людини і основних свобод [3], Рекомендація (2000) 21 Комітету Міністрів Ради Європи про свободу професійної діяльності адвокатів [27], Основні положення ООН про роль адвоката (далі – «Основні положення») і т. ін.) [22]. Так, п. 22 Основних положень передбачає, що уряди повинні визнавати і додержуватися конфіденційності комунікацій і консультацій між адвокатом і клієнтом у межах відносин щодо виконання адвокатом своїх професійних обов'язків[4]. Закон України «Про адвокатуру та адвокатську діяльність» від 05.07.2012 р., № 5076-VI (далі – Закон № 5076-VI) визначає **адвокатську таємницю** як будь-

[4] *Примітка. Основні положення встановили, що уряди забезпечують адвокатам: а) можливість здійснювати професійні обов'язки без залякування, перешкод, завдання турботи й недоречного втручання; б) можливість вільно пересуватися і консультувати клієнта у своїй країні та за кордоном; в) неможливість піддавати покаранню або погрожувати його застосуванням та можливості обвинувачення, адміністративних, економічних та інших санкцій за дії, здійснювані відповідно до визнаних професійних обов'язків, стандартів та етичних норм Обов'язком влади є забезпечення адвокату можливості своєчасно знайомитися з інформацією, документами і матеріалами справи, аби мати можливість надавати ефективну правову допомогу клієнтам (Див.: Основні положення про роль адвокатів (Див.: Прийняті VIII Конгресом ООН по запобіганню злочинам у серпні 1990 року. – URL: http://zakon2.rada.gov.ua/laws/show/995_835).*

яку інформацію, що стала відома адвокату, помічнику адвоката, його стажисту, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, й питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених законом підстав) звертався до адвоката, адвокатського бюро або об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, а також інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності [22].

Адвокатська діяльність є яскравим прикладом соціологічної професії, що передбачає активну взаємодію з людьми, й належить до професії типу «людина – людина», що ґрунтується на зборі, обробці, використані, зберіганні та поширенні значної за обсягом і різної за змістом інформації, яка потребує комплексного захисту організаційно-технічними та правовими засобами Водночас, за своєю природою, адвокатська таємниця не є абсолютною і за певних умов може бути обмежена. Інформація може втратити статус таємниці за письмовою заявою клієнта. Лише інформація щодо клієнта, з яким у адвоката укладено договір про надання допомоги, захищається режимом адвокатської таємниці, а дані щодо третіх осіб захищаються законодавством щодо захисту персональних даних, тобто правовим режимом конфіденційної інформації.

Адвокат, адвокатське бюро, адвокатське об'єднання, зобов'язані забезпечити умови, що унеможливлюють доступ сторонніх осіб до таємниці або її розголошення. З огляду на це, на адвоката покладаються такі обов'язки, як: дотримуватися присяги та правил адвокатської етики; повідомляти клієнта про виникнення конфлікту інтересів; без згоди клієнта не розголошувати адвокатську таємницю, не використовувати її у своїх інтересах або інтересах третіх осіб тощо [22]. Реалізувати ці обов'язки дозволяють встановлені Законом № 5076-VI заборони, зокрема, на: втручання і перешкоди здійсненню адвокатської діяльності; вимагання від адвоката, його помічника, стажиста, особи, яка перебуває у трудових відносинах з адвокатом, адвокатським бюро або об'єднанням, а також від особи, щодо якої припинено або зупинено право на заняття адвокатською діяльністю (далі – «носії таємниці»), надання відомостей, що є таємницею. З цих питань носії таємниці не допитуються, крім випадків, звільнення їх від обов'язку зберігати таємницю клієнтом, а ОРЗ чи слідчі дії здійснюються виключно з дозволу суду, на підставі судового рішення, ухваленого за клопотанням Генпрокурора, його заступників, прокурора АРК, області, міст Києва та Севастополя. Забороняється проведення огляду, розголошення, витребування чи вилучення документів, пов'язаних із адвокатською діяльністю, а також залучення адвоката до конфіденційного співробітництва у процесі ОРЗ чи слідчих дій, якщо таке співробітництво буде пов'язане або може призвести до розкриття адвокатської таємниці; окремо забороняється втручання у приватне спілкування адвоката з клієнтом тощо [22]. Задля дотримання цих гарантій встановлена кримінальна відповідальність у низці статей: 374, 397, 398, 399 КК, ст. 400 КК України [11].

Втім, аналітичні і статистичні дані свідчать про активну протидію адвокатам з метою утруднення чи повного блокування їх діяльності, що виявляється у недопущені адвоката до підзахисного під час проведення слідчих (розшукових) дій, ототожнені клієнта з адвокатом, наслідком чого є підозра захисника у пособництві або співучасті у вчиненні злочину, виклик і допит як свідка адвоката в кримінальному провадженні, в якому останній є захисником. Дані Єдиного звіту про кримінальні правопорушення за січень-грудень 2016 року [3] свідчать, що за вказаний період було вчинено: 4 злочини, кваліфіковані за ст. 374 КК; 55 правопорушень – за ст. 397 КК, з яких жодного не направлено з обвинувальним актом до суду; 31 – кваліфіковані за ст. 398 КК, з яких до суду направлено 2. Цікавим виглядає рядок ст. 400 «Посягання на життя захисника чи представника особи у зв'язку з діяльністю, пов'язаною з наданням правової допомоги» КК України, адже в останньому не відображено жодного факту, пов'язаного з посяганням на життя адвокатів, що реально мали місце. Зокрема, «Звіт про порушення прав адвокатів та гарантій адвокатської діяльності в Україні 2013-2016» дає такі дані про злочини вчинені відносно адвокатів: вбивства та посягання на життя (2 і 1 випадок відповідно у 2015 р., 2 вбивства у 2016 р.); кримінальне переслідування (3 і 2 випадки у ті самі роки, відповідно); фізична розправа (3 випадки у 2015 і 2016 рр.); погрози (3 і 2 випадки у ті самі роки відповідно); знищення майна (3 випадки у 2015 і 2016 рр.); обшуки (5 випадків у 2015 і 2016 рр.); здійснення НС(Р)Д (3 і 1 випадків у ті ж роки) та ін. Отримання адвокатами погроз, насильство над ними, незаконні обшуки, внаслідок яких вилучаються джерела адвокатської таємниці, є результатом активного представництва інтересів клієнтів і свідчить про нівелювання принципу адвокатської діяльності – *заборони ототожнення адвоката та клієнта* [6]. Такий стан справ викликає занепокоєння щодо реальності відображення стану дотримання прав адвокатів і гарантій їх діяльності, й ефективності досудового розслідування та судового розгляду кримінально караних порушень відносно них.

Протидія адвокатами гостро відчувається у процесі кримінального провадження, зокрема на досудовому розслідуванні. Так, проведення С(Р)Д з порушенням підстав і порядку, які встановлено КПК України (незаконні обшуки, вилучення джерел адвокатської таємниці, допити адвокатів з питань, які захищаються професійною таємницею), порушує не лише професійні права захисників, але й права підозрюваних (обвинувачених) на захист, унеможливлюючи його. Згідно з ч. 5 і 6 ст. 46 КПК України захисник має право брати участь у допиті та інших процесуальних діях, що проводяться за участі підозрюваного, обвинуваченого, до першого допиту підозрюваного мати з ним *конфіденційне побачення без дозволу слідчого, прокурора, суду*, а після першого допиту – такі ж побачення без обмеження кількості та тривалості. Ці зустрічі можуть відбуватися під візуальним контролем службової особи, але за виключенням прослуховування чи підслуховування. Документи, пов'язані з виконанням захисником його обов'язків, без його згоди не підлягають огляду, вилученню чи розголошенню слідчим, прокурором, слідчим суддею, судом [9]. Захисник зобов'язаний, без згоди підозрюваного, обвинуваченого не розголошувати відомості, які стали відомі у зв'язку з участю в кримінальному провадженні, які становлять адвокатську або іншу охоронювану таємницю [10].

Особливою гарантією збереження адвокатської таємниці є заборона, що передбачена ч. 2 ст. 275 КПК України, – залучення до конфіденційного співробітництва під час проведення НС(Р)Д адвоката, якщо таке співробітництво буде пов'язане з розкриттям конфіденційної інформації професійного характеру, під загрозою визнання недопустимими отримані докази [11, с. 694]. Втім такі гарантії порушуються. Незаконна протидія адвокатській діяльності відбувається, зокрема, за допомогою реєстрації відносно адвокатів відомостей у ЄРДР, з подаль-

шою можливістю здійснення С(Р)Д щодо нього (наприклад, обшуку). Провадження слугує прикриттям інформаційної розвідки органів досудового розслідування щодо певного клієнта адвоката, що унеможливлює захист.

Стаття 30 Конституції України не допускає проникнення до житла чи до іншого володіння особи, проведення в них огляду чи обшуку інакше як за вмотивованим рішенням суду. Так, ст. 8 Європейської конвенції про захист прав людини і основоположних свобод від 04.11.1950 р. встановлює, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Чинне законодавство України передбачає, що, у разі проведення обшуку чи огляду житла, іншого володіння адвоката, приміщень, де він здійснює адвокатську діяльність, тимчасового доступу до речей і документів адвоката слідчий суддя, суд у своєму рішенні в обов'язковому порядку зазначає перелік речей, документів, що планується відшукати, виявити чи вилучити під час проведення слідчої дії чи застосування заходу забезпечення кримінального провадження. Під час проведення обшуку чи огляду житла, іншого володіння адвоката, приміщень, де він здійснює адвокатську діяльність, тимчасового доступу до речей і документів адвоката має бути присутній представник ради адвокатів регіону. Для забезпечення його участі службова особа, яка буде проводити відповідну слідчу дію чи застосовувати захід забезпечення кримінального провадження, завчасно повідомляє про це раду адвокатів регіону за місцем проведення такої процесуальної дії [22]. Неявка останнього при завчасному повідомленні, не перешкоджає проведенню процесуальної дії [22]. Втім, часто службові особи правоохоронних органів зловживають оціночною категорією «завчасно», й здійснюють повідомлення за дуже незначний часовий період.

Такий стан справ є не лише грубим порушенням вітчизняного законодавства, але й нехтування принципами, які визнаються та гарантуються цивілізованих країнах. Зауважимо, що нині внесено зміни до чинного КПК України, зокрема Законом України «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування» від 16.11.2017 р., № 2213-VIII. Так, встановлено, що нині мають визнаватися судом недопустимими докази отримані під час виконання ухвали про дозвіл на обшук житла чи іншого володіння особи у зв'язку з недопущенням адвоката до цієї слідчої (розшукової) дії. Факт недопущення до участі в обшуку адвокат зобов'язаний довести в суді під час судового провадження (ч. 3 ст. 87 КПК). Право безперешкодного фіксування проведення обшуку за допомогою відеозапису, надається стороні захисту (ч. 1 ст. 107 КПК), що, безумовно, є суттєвим покращенням ситуації.

Повертаючись до питань обшуків саме у адвокатів, зауважимо, що нині сформована практика ЄСПЛ щодо проведення обшуків у приміщеннях, які належать адвокату, що може бути ефективно застосована. Зокрема, пп. 62, 63 рішення ЄСПЛ «Головань проти України» встановлюють, що присутність та дійова участь незалежного спостерігача завжди повинні бути доступними під час обшуку офісу адвоката для забезпечення того, щоб матеріал, який захищається адвокатською таємницею, не було вилучено. Спостерігач повинен мати юридичну кваліфікацію та повноваження, щоб бути спромог-ним запобігти втручанню в таємницю [20]. Це дозволяє забезпечити справедливий підхід до приватних і публічних інтересів і захисту адвокатської таємниці, що сприяє утвердженню принципу верховенства права та довіри до діяльності правоохоронних органів.

Виток адвокатської таємниці можливий внаслідок дії різних загроз. Нині, індустрія інформаційної безпеки розвивається у напрямку протидії зовнішнім загрозам, які утворились у зв'язку з розвитком ІТ, і чим ефективнішою є боротьба з ними, тим актив-ніше модернізуються внутрішні загрози інформаційної безпеки, на які припадає 70% усіх інцидентів[5]. Тому дослідження природи внутрішніх, зовнішніх і змішаних загроз інформаційної безпеки адвокатської діяльності має стати підгрунтям для розбудови системи криміналістичних методик розслідування окремих груп, підгруп, видів і підвидів злочинів, відносно інформаційної безпеки особи, суспільства і держави, й має сприяти систематизації останніх [2, с. 5-10]. Відповідно, розголошення адвокатської таємниці можливе внаслідок недоліків забезпечення інформаційної безпеки такої діяльності на рівні *інформаційних ресурсів, інформаційної інфраструктури та інформаційного поля*[6]. Аналізуючи стан забезпечення інформаційної безпеки адвокатської діяльності, можливо виокремити недоліки у забезпечені інформаційної безпеки, які сприяють витоку інформації. Недоліки у забезпеченні безпеки «інформаційних ресурсів»[7] адвокатської діяльності, включають прорахунки в організації конфіденційного діловодства, кадрового, інформаційно-аналітичного та матеріально-технічного забезпечення безпеки інформаційних ресурсів. Організаційні заходи забезпечення інформаційної безпеки є найбільш вразливими [9]. Не дивлячись на суттєві досягнення у галузі програмного забезпечення із запобігання витокам конфіденційної інформації, величезна кількість випадків «компрометування даних» (порушення їх конфіденційності), пов'язано саме з паперовими джерелами. Отже, проблема полягає не стільки у відсутності певних засобів захисту інформації, скільки у недостатній регламентації порядку роботи працівників з паперовими джерелами, і низькій обізнаності у галузі забезпечення інформаційної безпеки, що є суттєвим недоліком організаційної складової захисту інформації [9]. Необізнаність працівників, породжує їх недбале поводження з джерелами таємниці, що обумовлює необхідність ретельного добору, підготовки та інструктажу кадрів до функціональних обов'язків яких, буде входити збір і опрацювання інформації. Маємо враховувати й психологічні особливості інсайдера – носія адвокатської таємниці. Особливістю адвокатської діяльності є взаємодія

[5] *Примітка. Результати досліджень проведених Computer Security Institute (CSI) спільно з Federal Bureau of Investigation (FBI) США свідчать, що співвідношення зовнішніх і внутрішніх загроз становить 62% та 48% відповідно. За оцінками CSI та FBR обсяг втрат від витоків інформації з обмеженим доступом складає більше 70 мільйонів доларів США, що випередило віруси (27 млн. доларів США), хакерські атаки (65 млн. доларів США), фінансові шахрайства (10 млн. доларів США). Середній розмір втрат від дій інсайдерів склав 300 тис. доларів США. (Див.: 2010/2011 Computer Crime and Security Survey: 15th annual report by the CSI. – URL : https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf.*

[6] *Примітка. Розуміння інформаційної безпеки в аспекті забезпечення безпеки інформаційних ресурсів, безпеки інформаційної інфраструктури, а також безпеки «інформаційного поля» було запропоновано А. І. Марущаком у дослідженні проблем забезпечення інформаційної безпеки банків. (Див.: Марущак, А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези. доп. на Міжнар. наук-практ. .конф. (м. Севастополь, 1–2 жовтня 2010 р.). – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21–24).*

[7] *Примітка. Інформаційні ресурси установи – взаємопов'язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація, яка або була надана або належить їй (Див.: Марущак, А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези. доп. на Міжнар. наук-практ. .конф. (м. Севастополь, 1–2 жовтня 2010 р.). – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21–24).*

з людьми, що передбачає активну комунікацію та отримання значного масиву даних, що нерідко викликає у працівника особливий психологічний стан, – «**емоційного вигорання**» [18][8].

Окремою проблемою, яка сприяє витоку інформації є відсутність спеціального діловодства або неналежна організація та контроль за виконанням його вимог. Йдеться про внутрішні положення, які визначають правила здійснення діловодства в адвокатській діяльності як самозайнятих адвокатів, так і адвокатських бюро, об'єднань, юридичних фірм. Нині доцільно розробляти положення щодо формування, введення, зберігання та знищення адвокатських досьє, які затверджуються наказом (розпорядженням) керівника та доводяться до відома працівників під розпис. Ці положення передбачають строки, порядок зберігання та утилізації інформації з обмеженим доступом, яка захищається правовим режимом адвокатської таємниці. Недбале ведення досьє, журналів з реєстрації вхідної та вихідної інформації, журналів з реєстрації адвокатських запитів тощо, сприяє неконтрольованому витоку таємниці. Окрім того, досьє, у сучасних умовах систематичного порушення професійних прав адвокатів, є превентивним заходом неконтрольованого витоку інформації. Досьє є засобом збереження таємниці, оскільки законодавством України забороняється проведення огляду, розголошення, витребування чи вилучення документів, пов'язаних із здійсненням адвокатської діяльності, а у разі порушення цих вимог відомості та матеріали, які містяться в досьє, не можуть бути використані як докази при формуванні повідомлення про підозру чи обвинувачені.

Досьє відображає стратегію і тактику допомоги, захисту та представництва клієнта адвокатом у певній справі, яка грунтується на фактичних обставинах й враховує позиції сторін. Організацію та контроль за введенням досьє здійснює особа у провадженні якої перебуває справа або особа, визначена наказом керівника, яка забезпечує збереження та оперативне оновлення змісту досьє. Формування адвокатських досьє відбувається у паперовій формі та в електронно-цифровому вигляді, у процесі створення автоматизованого робочого місця (далі – АРМ) носіїв адвокатської таємниці захист яких має бути надійно забезпечений на організаційно-кадровому та матеріально-технічному рівні. Коли адвокат вступає до справи, яка вже певним чином об'єктивувалась у досудовому чи судовому провадженні, останній ознайомиться з наявними матеріалами для чого, завжди, здійснюється матеріальне або електронно-цифрове копіювання справи, що нерідко містить відомості не лише щодо клієнта, але й окремих органів державної влади, їх посадових осіб, підприємств, установ або організацій, їх посадових осіб та інших громадян, які потрапили до орбіти правового конфлікту. Носії адвокатської таємниці зобов'язані забезпечити достатні умови збереження цілісності і конфіденційності досьє, документів і речових доказів, отриманих у процесі допомоги[9].

Другим рівнем інформаційної безпеки адвокатської діяльності є рівень забезпечення **безпеки інформаційної інфраструктури**[10], що включає недоліки та прорахунки у функціонуванні і забезпеченні безпеки використання ІТ адвокатами, зокрема, засобів обчислювальної техніки (ПК), їх програмного забезпечення, телекомунікаційних засобів зв'язку. Так, сприяють розголошенню адвокатської таємниці: відсутність або незадовільний стан технічних засобів забезпечення безпеки інформаційної інфраструктури; фрагментарність або несправність засобів захисту, технічного і програмного середовища; відсутність криптографічного захисту для інформації під час її обробці ЕОМ, системах та мережах ПК і електрозв'язку об'єднання; відсутність ідентифікації користувача та здійснюваних ним операцій за допомогою паролів, ключів; відсутність відображення дати та часу дій користувачів з інформаційними та програмними ресурсами у ЕОМ, комп'ютерних мережах, протиправних спроб доступу до них; відсутність програмного забезпечення, що розпізнавало б передачу інформації незахищеними лініями зв'язку [17, с. 23][11].

Зауважимо, що розголошенню таємниці сприяють й інші недоліки у забезпеченні безпеки інформаційних ресурсів, зокрема, недостатній рівень обмеження доступу сторонніх осіб до приміщень, в яких обробляється (зберігається) інформація з обмеженим доступом (наприклад, архів); відсутність заходів контролю за роботою працівників із носіями таємниці; низький рівень дисципліни та професійна деформація працівників; відсутність ефективної системи виявлення та реагування на протиправні дії відносно таємниці; ненадійна система охорони та зберігання джерел інформації (неналежний технічний стан сейфів тощо), що не виключає можливість ознайомлення з нею.

Окремої популярності серед адвокатів набули месенджери, – програми швидкого обміну повідомленнями, розроблені для оперативного спілкування за допомогою мережі Інтернет. Месенджери дозволяють обмінюватися текстовими файлами, здійснювати голосовий і відеозв'язок, а також обмінюватися файлами. Нині популярні Skype, WhatsApp, ICQ, Viber, Telegram, Line, Facebook Messenger тощо, кожен з яких має особливості із захисту інформації та положення про конфіденційність, і кожне з яких не раз піддавалося хакерським атакам, внаслідок чого відбувався виток інформації. Не варто забувати й про можливості контрольованого зняття інформації з каналів зв'язку.

Третій рівень включає недоліки в безпеці «**інформаційного поля**» адвокатської діяльності, який утворюється з несистематизованих потоків інформації, що оприлюднюються різними учасниками інформаційних відносин (телерадіоорганізаціями, ЗМІ) [17, с. 23]. Втім, адвокат може, за погодженням з клієнтом, умисно передає певну інформацію до ЗМІ, що становить частину обраної стратегії захисту прав і представництва інтересів клієнта, та становить контрольований виток таємниці, що є допустимим[12].

---

[8] *Примітка. Емоційне вигорання виявляється у таких професійних деформаціях: професійна індиферентність (передбачає прояв байдужості, емоційної сухості, жорстокості), негативного сприйняття етичних норм і правил поведінки (Див.: Зеер Э.Ф. Психология профессий : учеб. пособ. –2-е изд., перераб., доп. – М. : Деловая книга, 2003. – С. 114–115).*

[9] *Примітка. На них розміщується напис: «У сейфі зберігаються джерела інформації, яка становить адвокатську таємницю. Проведення огляду, розголошення, витребування чи вилучення документів, пов'язаних із здійсненням адвокатської діяльності забороняється (п. 4 ч. 1 ст. 23 Закону України № 5076-VI). За порушення встановлених законом гарантій адвокатської таємниці винні особи несуть кримінальну відповідальність (ст. 397 КК України)».*

[10] *Примітка. Безпека інформаційної інфраструктури передбачає стан захищеності ПК, систем та комп'ютерних мереж і мереж електрозв'язку, що забезпечують цілісність і доступність інформації, що в них обробляється (Див.: Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. на Міжнар. наук-практ. конф. (м. Севастополь, 1–2 жовтня 2010 року). – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21).*

[11] *Примітка. Розпізнають передачу конфіденційної інформації незахищеними лініями зв'язку DLP-системи, які виявляють публікації в мережі Інтернет, під час аналізу матеріалів за допомогою пошукових систем шляхом формулювання до них кількох запитів, що містять ключові слова (Див.: Федотов Н.Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? – URL: http://forensics.ru/investigation_blogs.html).*

[12] *Примітка. М.М. Федоров пише, що приймати рішення про коректність інформації, що на-дається до ЗМІ, може лише уповноважена особа – піар-цензор, який не лише є відповідальним за попереднє ознайомлення працівників з існуючою внутрішньою цензурою, й реально контролює будь-яке спілкування із ЗМІ (Див.: Федотов, Н.Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? – URL: http://forensics.ru/investigation_ blogs.html).*

Висновки. Таким чином, інформаційна безпека адвокатської діяльності має специфічний характер через особливість цієї професійної діяльності, головним принципом якої є конфіденційність. Розголошення адвокатської таємниці передбачає порушення стану інформаційної безпеки адвокатської діяльності і включає недоліки у забезпеченні інформаційної безпеки на трьох самостійних рівнях, зокрема, на рівнях безпеки інформаційних ресурсів, безпеки інформаційної інфраструктури, а також безпеки «інформаційного поля». Це дозволяє комплексно проаналізувати різнорідні недоліки у забезпеченні інформаційної безпеки адвокатської діяльності, а також попередити у майбутньому неконтрольований виток інформації з обмеженим доступом.

Література:

1. Білоус В.В. Інформаційні технології у криміналістиці: постановка проблеми // Проблеми законності. – 2013. – Вип. 121. – С. 166.
2. Європейська конвенція про захист прав людини і основних свобод : Конвенція ратифікована Законом від 17.07.97 р., № 475/97-ВР [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_004.
3. Єдиний звіт про кримінальні правопорушення: форма № 1 (місячна), затв. наказом ГПУ від 23 жовтня 2012 р. № 100 за погодженням з Держстатом України Генеральною прокуратурою України. [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/stst2011.html?dir_id=112661&libid=100820.
4. Журавель В.А. Криміналістичні методики: сучасні наукові концепції : монографія В.А. Журавель. – Харків : Апостіль, 2012. – С. 122–123
5. Журин С.И. Инсайдер: основная характеристика и комплексность противодействия [Електронний ресурс] / С.И. Журин // Безопасность информационных технологий : науч. журнал ВНИИПВТИ. – 2011. – № 4. – С. 178. – Режим доступу : http://www.pvti.ru/articles_34.htm.
6. Захист прав адвокатів та гарантій адвокатської діяльності: заключення та рекомендації від 09 червня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.justicereformukraine.eu/wp-content/uploads/2016/06/Protecting AdvocatesMemo_FINAL_ukr.pdf.
7. Зеер Э.Ф. Психология профессий : учеб. пособ. / Э.Ф. Зеер. – 2-е изд., перераб., доп. – М. : Деловая книга, 2003. – С. 114–115.
8. Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России в 2012 году : отчет об уровне зашиты конфиденциальных данных. – 2013. – С. 13. [Електронний ресурс]. – Режим доступу : http://www.infowatch.ru/node/3013?sid=5358.
9. Конституція України: Закон України від 28 червня 1996 року, 254к/96-вр. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
10. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012, № 4651-VI. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/4651-17/page.
11. Кримінальний процесуальний кодекс України: наук.-практ. коментар : у 2 т. / Національна академія правових наук України ; ред.: В.Я. Тація, В.П. Пшонки. – Харків : Право, 2012. – Т. 1. – С. 694.
12. Кримінальний кодекс України : Закон України від 05 квітня 2001року, № 2341-III. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14/page11.
13. Крылов В.В. Расследование преступлений в сфере информации: монографія / В.В. Крылов. – М. : Изд-во «Городец», 1998. – С. 164.
14. Марущак А.І. Інформаційна безпека банківської установи: структура та система забезпечення : тези. доп. на Міжнар. наук-практ. конф. (м. Севастополь, 1–2 жовтня 2010 р.). / А.І. Марущак.– Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21–24.
15. Основні положення про роль адвокатів : Прийняті VIII Конгресом ООН по запобіганню злочинам у серпні 1990 року. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_835.
16. Островська М. Практика ЄСПЛ в контексті обшуків у адвокатів : стаття / Марія Островська // Юридичний вісник – 2016– № 33. [Електронний ресурс]. – Режим доступу : http://unba.org.ua/publications/print/1730-praktika-espl-v-konteksti-obshukiv-u-advokativ.html.
17. Петрик В. Сутність інформаційної безпеки держави, суспільства та особиВ. Петрик. // Юстиніан : електрон. наук. фахове вид. – 2009. – Вип. 5. [Електронний ресурс]. – URL : http://www.justinian.com.ua/article.php?id=3222.
18. Про адвокатуру та адвокатську діяльність: Закон України від 5 липня 2012року, № 5076-VI. [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/5076-17.
19. Резнікова Г. І. Криміналістична характеристика злочинів щодо розголошення професійних таємниць : автореф. дис. ... канд. юрид. наук. – Харків, 2015. – 20 с.
20. Про свободу професійної діяльності адвокатів : Рекомендація № R (2000) 21 Комітету Міністрів. 2000. – 25 жовтня. [Електронний ресурс]. – Режим доступу : www.scourt.gov.ua/clients/vsu/.../Рекомендація%20№%20R%20(2000)%2021.doc.
21. Russia's military on Thursday revealed plans for a United Nations-backed plan for a global non-aggression pact, banning cyberwarfare attacks in peacetime between all leading powers. [Електронний ресурс]. – URL : http://sputniknews.com/science/20160204/1034202933russia-militarycyberwarfare-nonaggression.html.
22. Федотов Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М. : Юрид. Мир, 2007. – 432 с.
23. Федотов, Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Електронний ресурс]. / Н.Н.Федотов. – Режим доступу : http://forensics.ru/investigation_ blogs.html.
24. Филатова О. Как Израилю удается бороться с терроризмом с помощью соцсетей [Електронний ресурс]. / О. Филатова. – Режим доступу: http://uinp.info.

Резникова А. И. Информационная безопасность адвокатской деятельности: криминалистический взгляд

Аннотация. Нарушение состояния информационной безопасности адвокатской деятельности возможно вследствие существования внутренних, внешних и смешанных угроз. Первым классом угроз информационной безопасности являются внутренние угрозы адвокатской деятельности, то есть незаконная деятельность инсайдеров (адвокатов, их помощников, стажеров, лиц, находящихся в трудовых отношениях с адвокатом, адвокатским бюро, адвокатским объединением, а также лиц, в отношении которых прекращено или приостановлено право на занятие адвокатской деятельностью). Второй класс угроз информационной безопасности адвокатской деятельности составляют внешние угрозы киберпространства вирусы, сетевые черви, руткиты клавиатурные шпионы. Третий класс – смешанные формы угроз, то есть объединение усилий внешних и внутренние нарушителей информационной безопасности.

Ключевые слова: адвокатская тайна, информационные ресурсы, информационное поле, информационная инфраструктура, адвокатское досье.

Reznikova H. Information security of advocacy: a criminalistic view

Summary. Violation of the state of information security of the advocacy may be due to the existence of internal, external and mixed threats. The first class of threats to information security is the internal threats of lawyer activity, that is, the illegal activities of insiders (lawyers, their assistants, trainees, persons in labor relations with a lawyer, law office, lawyer's association, as well as persons who are suspended or stopped the right to practice advocacy). The second class of threats to information security attorney activities are external threats to cyberspace viruses, network worms, phishing, vinsing, hacking attacks, etc. Third class are mixed forms of threats, that is, the combination of efforts of external and internal violators of information security.

Key words: advocacy, lawyer's secret, lawyer's dossier,informational security, information resources, information field,information infrastructure.