УДК 342.11
DOI https://doi.org/10.32782/2524-0374/2024-11/113

ДЕЯКІ ПИТАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ

SOME QUESTIONS REGARDING INFORMATION SECURITY IN ADVOCACY

Гафич І.І., адвокат, д.філос. у гал. права,
асистент кафедри прав людини та юридичної методології
Національний юридичний університет імені Ярослава Мудрого

У сучасному світі, де інформаційні технології відіграють ключову роль у всіх сферах життя, питання інформаційної безпеки стає надзвичайно актуальним для адвокатів. Адвокатська діяльність передбачає роботу з великою кількістю конфіденційної інформації, яка потребує надійного захисту від несанкціонованого доступу, розголошення та втрати. У статті автор аналізує основні аспекти інформаційної безпеки адвоката, включаючи фізичну, технічну та організаційну безпеку, а також способи збереження даних.

Автор розглядає фізичну безпеку, яка охоплює заходи щодо захисту офісних приміщень, де зберігаються документи та електронні носії, такі як встановлення систем відеоспостереження, сигналізації та використання сейфів. Технічна безпека включає використання шифрування для захисту електронних даних, встановлення антивірусного програмного забезпечення та фаєрволів, а також регулярне оновлення програмного забезпечення для усунення вразливостей. Організаційна безпека передбачає впровадження політик та процедур щодо збереження конфіденційності, навчання персоналу щодо правил безпеки та конфіденційності.

Автор також аналізує способи збереження даних адвоката, які включають шифрування даних, регулярне створення резервних копій, впровадження системи контролю доступу до конфіденційної інформації, використання двофакторної аутентифікації, а також спеціалізованого програмного забезпечення для захисту від кіберзагроз. Документування та моніторинг дій користувачів у системі дозволяють виявляти підозрілу активність та запобігати можливим загрозам.

У статті автор наводить приклади практичних заходів, які можуть бути використані для забезпечення високого рівня захисту адвокатської таємниці та конфіденційної інформації клієнтів. Зокрема, розглядаються такі заходи, як встановлення біометричних замків, використання програмного забезпечення для шифрування електронної пошти, впровадження політики конфіденційності та проведення тренінгів для співробітників.

Таким чином, автор робить висновок, що забезпечення інформаційної безпеки адвоката є комплексним процесом, що вимагає застосування різноманітних заходів та інструментів. Впровадження ефективних заходів безпеки дозволяє адвокатам захищати конфіденційну інформацію клієнтів, зберігати довіру та забезпечувати високий рівень професійної діяльності.

Ключові слова: інформаційна безпека, захист даних, адвокатура технології безпеки, кіберзагрози, методи захисту, кібербезпека, шифрування, аутентифікація, управління ризиками, безпека мережі.

In the modern world, where information technologies play a key role in all spheres of life, the issue of information security becomes extremely relevant for lawyers. Legal activity involves working with a large amount of confidential information that requires reliable protection against unauthorized access, disclosure and loss. In the article, the author analyzes the main aspects of a lawyer's information security, including physical, technical, and organizational security, as well as ways to save data.

The author considers physical security, which covers measures to protect office premises where documents and electronic media are stored, such as the installation of video surveillance systems, alarms and the use of safes. Technical security includes using encryption to protect electronic data, installing anti-virus software and firewalls, and regularly updating software to address vulnerabilities. Organizational security involves the implementation of privacy policies and procedures, training of personnel on security and privacy rules.

The author also analyzes the methods of protecting the lawyer's data, which include data encryption, regular backups, implementation of a system of access control to confidential information, the use of two-factor authentication, as well as specialized software for protection against cyber threats. Documenting and monitoring user actions in the system allows you to detect suspicious activity and prevent possible threats.

In the article, the author provides examples of practical measures that can be used to ensure a high level of protection of attorney secrecy and confidential information of clients. In particular, measures such as the installation of biometric locks, the use of email encryption software, the implementation of a privacy policy and training for employees are being considered.

Thus, the author concludes that ensuring a lawyer's information security is a complex process that requires the use of various measures and tools. Implementation of effective security measures allows lawyers to protect confidential client information, maintain trust and ensure a high level of professional activity.

Key words: information security, data protection, security technology law, cyber threats, protection methods, cyber security, encryption, authentication, risk management, network security.

Постановка пробеми: В умовах швидкого технологічного прогресу та всепроникності інформаційних технологій, захист даних стає критично важливим завданням. Особливо це стосується адвокатської діяльності, яка передбачає роботу з великою кількістю конфіденційної інформації клієнтів. Адвокати зобов'язані забезпечувати збереження адвокатської таємниці, що вимагає впровадження ефективних заходів інформаційної безпеки. Основні проблеми, які постають перед адвокатами у сфері інформаційної безпеки, включають: захист конфіденційної інформації, кіберзагрози, фізичну безпеку, організаційні заходи та технічні засоби захисту. Адвокати працюють з чутливими даними, які можуть бути цікавими для зловмисників. Витік такої інформації може призвести до серйозних наслідків як для клієнтів, так і для самого адвоката. З розвитком технологій зростає кількість кіберзагроз, таких як фішинг, віруси, шкідливе програмне забезпечення та інші види атак. Адвокати повинні бути готові до захисту своїх систем від таких загроз. Окрім кіберзагроз, важливим є також захист фізичних носіїв інформації, таких як паперові документи та електронні носії. Необхідно забезпечити надійний захист офісних приміщень та місць зберігання документів. Впровадження політик та процедур щодо збереження конфіденційності, навчання персоналу та контроль доступу до інформації є важливими аспектами забезпечення інформаційної безпеки.

Використання сучасних технологій, таких як шифрування, антивірусне програмне забезпечення, фаєрволи та системи моніторингу, є необхідним для захисту електронних даних. Таким чином, проблема інформаційної безпеки адвоката є комплексною і вимагає всебічного підходу. Необхідно розробити та впровадити ефективні заходи захисту, які б забезпечували надійне збереження конфіденційної інформації клієнтів та відповідали сучасним викликам у сфері інформаційної безпеки. У статті автор аналізує ці проблеми та пропонує практичні рішення для їх подолання, що дозволить адвокатам забезпечити високий рівень захисту інформації та зберегти довіру клієнтів.

Метою цієї статті є дослідження та аналіз сучасних методів захисту інформації в умовах стрімкого розвитку технологій. Стаття спрямована на визначення основних загроз інформаційній безпеці в сучасному світі для адвоката, огляд існуючих технологій та методів захисту даних, включаючи їх переваги та недоліки, аналіз ефективності різних підходів до захисту інформації в різних галузях, а також розробку рекомендацій щодо покращення інформаційної безпеки. Ця стаття має на меті надати глибоке розуміння актуальних проблем інформаційної безпеки адвоката та можливих шляхів їх вирішення.

Виклад основного матеріалу. Адвокат є головним суб'єктом дотримання конфіденційності при наданні правничої допомоги, комунікації з правоохоронними органами, органами державної влади тощо. Клієнти віддають перевагу захисту конфіденційної інформації через дію адвокатської таємниці, яка забезпечує особливо високий рівень захисту, зокрема завдяки гарантіям, що захищають адвокатську діяльність від втручань. Вони використовують послуги адвокатів (або інших форм адвокатської діяльності) для зберігання документів, включаючи ті, що мають електронний формат.

Інформаційні технології чинять значний вплив на правове середовище, наприклад, цифровізація дозволяє адвокату скоріше ознайомитися з матеріалами справи, скануючи їх та переносячи на електронні носії; відтворювальні пристрої (звукозапис) спрощують нотування важливих деталей в ході судового засідання, та можливість переслухати запис для формування якісної та ефективної лінії захисту; USB – накопичувачі та жорсткі диски дають змогу в будь-який момент скористатися інформацією, не турбуючись про різноманітні фактори впливу та ін. Проте, інформаційні технології, не дивлячись на їхню користь, несуть певні загрози: віруси, дезінформацію, дестабілізацію комп'ютерних систем адвоката, що нейтралізує його роботу на певний час. Тому об'єктом нашого дослідження є висвітлення механізмів та способів правового регулювання збереження інформаційної недоторканності адвоката.

Питання зберіганню адвокатської таємниці залишається актуальним і нині, особливу увагу врегулюванню цього аспекту правничої допомоги приділяли: міжнародна спільнота та представники юридичних професій щодо регламентації та стійкості на позиції забезпечення принципу конфіденційності відносин адвоката з клієнтом. Такі правові та етичні аспекти адвокатської діяльності мають строго захищатися законом.

Говорячи про міжнародні стандарти, які регламентують питання адвокатської таємниці, то варто зазначити такі акти:

– Рекомендація № R (2000) Комітету міністрів державам – членам Ради Європи про свободу здійснення професії адвоката. У 3 принципі п. 2 зазначено, що обов'язок збереження професійної таємниці покладено на адвокатів відповідно до законів, підзаконних актів і професійних стандартів країни. Будь-яке порушення конфіденційності без згоди клієнта буде супроводжене відповідними санкціями.

– Загальний кодекс правил для адвокатів країн Європейської співдружності (1988 р.). Пункт 2.3 закріплює, що адвокат отримує конфіденційну інформацію від клієнта та зобов'язаний строго дотримуватися принципу конфіденційності. Це включає не лише відомості від клієнта, а й інші конфіденційні дані. Обов'язок збереження конфіденційності є безстроковим і розповсюджується на всіх осіб, які беруть участь у наданні юридичних послуг клієнту.

– Основні положення про роль адвокатів (1990 р.) – Уряди повинні визнавати та дотримуватися конфіденційності обміну інформацією та консультацій між адвокатом і клієнтом в контексті виконання адвокатських обов'язків.

– Мінімальні стандартні правила поводження з в'язнями («Правила Нельсона Мандели»). В ст. 93 говориться, що з метою захисту власних прав в'язні, що перебувають під слідством, мають право звертатися за безкоштовною юридичною консультацією та приймати в ув'язненні юридичного радника. Забезпечення цих прав передбачає надання письмового приладдя за їхньою вимогою, а зустрічі з юридичним радником повинні відбуватися під наглядом, але поза слухом міліцейських або в'язничних органів.

– Стандарти незалежної юридичної професії Міжнародної асоціації юристів. У ст. 12, 13 наголошується, що адвокати в справах осіб, позбавлених волі, повинні мати незалежність для забезпечення вільної та конфіденційної допомоги. Їм також слід надавати обладнання для ефективного виконання обов'язків, включаючи конфіденційність відносин, право на поїздки для консультацій та свободу пошуку, отримання та поширення інформації згідно з професійними нормами.

Важливим уточненням є те, що всі вищезазначені норми слугували фундаментом для формування сучасного українського законодавства.

Зокрема, Конституція проголошує ст. 131-2 незалежність адвокатури, засади її реалізації і діяльності визначаються законом. Гарантії конфіденційності адвокатської діяльності, знайшли своє відображення також в ст. 11 ЗУ «Про адвокатуру та адвокатську діяльність» (далі – Закон), а саме, адвокат присягає: «дотримуватися принципів верховенства права, законності, незалежності та конфіденційності…» [1], до того ж слідування вищезазначеним принципам регламентує ст. 21 Закону, що зобов'язує адвоката не розголошувати відомості, що становлять адвокатську таємницю. Ст. 22 Закону, безпосередньо, надає визначення адвокатській таємниці; інформацію, що можуть її становити; суб'єктів на яких поширюється обов'язок зберігати адвокатську таємницю тощо.

Аналогічні положення містяться й у Правилах адвокатської етики (далі – ПАЕ). Правила визначають принцип конфіденційності (ст. 10) як базову передумову довірчих відносин між адвокатом і клієнтом, без якої неможливе якісне надання правничої допомоги.

Отже, можна зробити проміжний висновок, що адвокату має гарантуватися безпечне, недоторкане «середовище» для збереження та утримання його інформації, наданої йому від клієнта чи отриманої в інший законний спосіб, іншими словами, ми маємо справу з інформаційною безпекою адвокатської діяльності. При цьому не має значення на якому носії зберігається ця інформація.

Не викликає заперечень той факт, що кіберобізнаність адвоката тісно пов'язана з етичною стороною адвокатської діяльності. Адже, обізнаність про кіберзагрози сприяє розвитку навичок для протидії їм, використовуючи продукти кібербезпеки. До прикладу, в Законі України «Про основні засади забезпечення кібербезпеки України» в ст. 4 наводиться вичерпний перелік об'єктів кібербезпеки та кіберзахисту. Одним з них є: «конституційні права, свободи людини і громадянина…» [2]. Тож, провівши системний аналіз норм Конституції, варто зазначити, що вони включають в себе: право особи на захист та заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди. Ст. 5 також визначає вичерпний перелік суб'єктів забезпечення кібербезпеки, йдеться про правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності. Як слушно зазначає Діордіца І.В., в своєму дослідженні, що нормативне закріплення адвокатури серед суб'єктів гарантування кібербезпеки сприяло б розвитку кібернетичної етики адвоката [3].

Інформаційна безпека є критично важливим аспектом сучасного суспільства, особливо в умовах зростаючих кіберзагроз та необхідності захисту конфіденційної

інформації адвоката та його клієнта. Для кращого розуміння цього поняття, важливо визначити основні терміни та рівні захисту, які використовуються в цій сфері. Наше розуміння включає такі основні поняття: **Інформаційна безпека** – це стан захищеності інформаційних ресурсів від несанкціонованого доступу, використання, розголошення, порушення цілісності або знищення. **Захист даних** – процеси та методи, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації. **Кібербезпека –** заходи, що спрямовані на захист комп'ютерних систем та мереж від кіберзагроз. **Шифрування** – метод захисту інформації шляхом перетворення її в нечитабельний формат, який може бути розшифрований лише за допомогою спеціального ключа. **Аутентифікація** – процес перевірки достовірності користувача або системи.

Щодо рівня захисту інформаційної безпеки, погоджуємося з Резніковой Г.І., що включає: **Рівень інформаційних ресурсів** – включає захист баз даних, файлів, документів та інших форм інформації. **Рівень інформаційної інфраструктури** – охоплює захист апаратного та програмного забезпечення, мережевих пристроїв та інших компонентів IT-інфраструктури. **Рівень інформаційного поля** – стосується захисту інформаційних потоків, комунікаційних каналів та засобів передачі даних. Ці рівні захисту є взаємопов'язаними та доповнюють один одного, забезпечуючи комплексний підхід до інформаційної безпеки.

До того ж, вчена наголошує, що проведений аналіз стану інформаційної безпеки в адвокатській діяльності виявив низку недоліків, які сприяють витоку конфіденційної інформації. Зокрема, проблеми в захисті інформаційних ресурсів адвокатської діяльності включають недоліки в організації конфіденційного діловодства, а також у кадровому, інформаційно-аналітичному та матеріально-технічному забезпеченні. Найбільш вразливими є організаційні заходи щодо забезпечення інформаційної безпеки. Незважаючи на значні досягнення в розробці програмного забезпечення для запобігання витокам конфіденційної інформації, значна кількість випадків компрометації даних пов'язана з паперовими джерелами [4].

На нашу думку, для підвищення рівня інформаційної безпеки в адвокатській діяльності необхідно впроваджувати комплексні заходи, які включають не лише технічні рішення, але й удосконалення організаційних процесів та підвищення обізнаності персоналу щодо важливості захисту інформації.

У своєму дослідженні Є.О. Колдов наголошує на гарантіях збереження адвокатської таємниці, особливо в аспекті проведення обшуків у адвокатів. При здійсненні обшуку або огляду приміщень адвоката та інших об'єктів його володіння, де здійснюється адвокатська діяльність, наявність представника ради адвокатів регіону є обов'язковою. Це необхідно для тимчасового доступу до речей і документів адвоката. У свою чергу, службова особа, яка проводить відповідні слідчі дії чи застосовує заходи забезпечення кримінального провадження, повинна заздалегідь повідомити Раду адвокатів регіону про здійснення такої процесуальної дії. При цьому неявка представника ради адвокатів регіону, за умови завчасного попередження, не перешкодає правоохоронним органам проводити слідчі дії [5]. Ми погоджуємося з думкою, що такі положення національного законодавства створюють плацдарм для процесуальних зловживань.

До прикладу, за даними НААУ в 2021 році в Україні зафіксовано 391 випадок затримання та обшуку адвокатів. З них 122 випадки стосувалися юристів з Київської області, а 95 – адвокатів міста Києва. На третьому місці за цим показником розташувалася Харківська область, де протягом року рада адвокатів регіону провела 38 виїздів на обшуки та затримання колег. [6]. При обшукі правоохоронні органи часто вдаються до вилучення сматфонів та інших гаджетів адвоката, проте існують певні обмеження щодо вилучення цих носіїв. Не викликає заперечень той факт, що робочі гаджети адвоката містять відомості, що становлять адвокатську таємницю. При проведені одного з таких обшуків адвокати Ю. Юрченко та Є. Солодко зафіксували порушення та зазначили їх в протоколі. Вилучаючи відомості з носія інформації представники правоохоронних органів можуть запропонувати виділити дані, що необхідні для розслідування, проте в даній ситуації метою було вилучення смартфону повністю.

Голова Комітету з питань захисту прав адвокатів та гарантій адвокатської діяльності також зауважив, що зобов'язання адвоката зберігати конфіденційність не обмежується часовими рамками і гарантується як на етапі прийняття завдання від клієнта та його виконання, так і після завершення виконання адвокатом угоди. Варто відзначити, що при прийнятті рішення про проведення обшуку слідчі судді не враховують законодавчих обмежень, пов'язаних із адвокатською таємницею, і дозволяють вилучати матеріали, чим порушують цей принцип. Таким чином нівелюються приписи законодавства, зокрема КПК України, адже, такі втручання службових осіб в діяльність адвоката вважаються злочином, за який передбачена відповідальність згідно зі статтею 397 Кримінального кодексу [7].

Практика ЄСПЛ свідчить наступне, зразковим є рішенням ЄСПЛ у справі «Ромен і Шміт проти Люксембургу». Згідно з текстом цього рішення, ЄСПЛ визначив, що при проведенні обшуку в офісі адвоката з метою виявлення джерел інформації його клієнта-журналіста порушено не лише право адвоката на приватне життя, згідно зі статтею 8 Конвенції, але також право його клієнта, яке гарантується статтею 10 Конвенції (свобода вираження поглядів). Крім того, у цьому рішенні суд вказав, що постанова про проведення обшуку була сформульована загальними термінами, що надавало широкі повноваження особам, які виконували обшук. Таке формулювання є спільним у всіх рішеннях ЄСПЛ стосовно обшуку в офісах адвокатів і є основною підставою для визнання порушення права адвоката, яке гарантується статтею 8 Конвенції (рішення у справах «Смирнов проти Російської Федерації», «Андре і інший проти Франції», «Манчевскі проти Молдови»).

Згідно з пунктами 62 і 63 Рішення у справі «Головань проти України», Європейський суд з прав людини визначив, що «необхідні гарантії, такі як участь та активна присутність незалежного спостерігача, завжди повинні бути забезпечені під час проведення обшуку в офісі адвоката. Це робиться для того, щоб матеріали, які захищаються адвокатською таємницею, не були вилучені. Такий спостерігач повинен обов'язково мати відповідну юридичну кваліфікацію для ефективної участі у процесі. Крім того, він зобов'язується зберігати адвокатську таємницю, забезпечуючи захист конфіденційного матеріалу та прав третіх осіб. Урешті-решт, спостерігач повинен мати необхідні повноваження для запобігання можливому втручанню в адвокатську таємницю під час здійснення процесуальних дій» [8].

З огляду на вищевикладене законодавець не поспішає врегульовувати дане питання, адвокат залишається у вразливому положенні, не маючи механізмів убезпечення своєї інформації від вилучення, викрадення тощо [9].

Важливим є уточнення, що в країнах-членах Європейського Союзу також на законодавчому рівні не врегульоване питання кібербезпеки адвоката. Проте, в Сполучених Штатах Америки існує Американське об'єднання юристів (American Bar Association – ABA). ABA була заснована в 1878 році з метою закласти правові та етичні основи американської нації. Сьогодні вона існує як членська організація та віддана своїй місії захисту свободи та досягнення справедливості. У 2017 році Постійний комітет з етики та професійної відповідальності ABA видав офіційний

висновок 477R, на предмет етичних зобов'язань адвоката щодо захисту конфіденційної інформації клієнта при передачі інформації, що стосується представництва через Інтернет. Цей висновок є оновленням офіційного висновку ABA 99-413 «Захист конфіденційності незашифрованої електронної пошти» (1999) [10].

Зокрема, в попередньому висновку йшлося про листування електронною поштою. Комітет визначив, що електронна пошта забезпечує розумне очікування конфіденційності, юристи можуть користуватися нею для комунікації зі своїми клієнтами. Такий підхід вважається законним, оскільки прослуховування телефонних розмов є так само незаконним, як і перехоплення електронної пошти. У той же час комітет визнає, що існує інформація, яка може бути настільки чутливою, що адвокат повинен розглядати можливість застосування особливо суворих заходів захисту, залежно від ступеня чутливості цієї інформації.

З моменту прийняття Рекомендації 99-413 відбулися значні зміни, особливо в сфері технологій та їх багатьох нових проявів, що активно розвиваються та широко використовуються в юридичній професії. Портативні комп'ютери, смартфони, соціальні мережі, хмарні сховища та Wi-Fi-з'єднання стали повсякденними реаліями, які значно еволюціонували з моменту опублікування Рекомендації. До того ж, стандарти професійної поведінки Американської асоціації юристів також зазнали ряду змін, зокрема, тих, що стосуються обов'язку юриста забезпечувати конфіденційність клієнта під час передачі інформації через Інтернет.

В оновленому виданні у параграфі 8 коментаря до правила 1.1 тепер зазначено, що «юрист повинен бути в курсі змін у законодавстві та його практиці, включаючи переваги та ризики технологій…». Також, було додано нову частину (c) до Правила 1.6, яка говорить: «Адвокат повинен докладати розумних зусиль, щоб запобігти випадковому або несанкціонованому розголошенню або несанкціонованому доступу до інформації, що стосується представництва інтересів клієнта.»

У Висновку 477R комітет ABA взяв до уваги зростаючу складність кіберзагроз у сучасному технологічному середовищі та визнав, що деякі нові форми електронного зв'язку, які стали звичайними, не завжди можуть забезпечувати розумне очікування конфіденційності та надав певні рекомендації щодо запобігання розголошення інформації. Серед них:

1. Розуміти природу загрози. Адвокати мають оцінювати кожну інформацію надану йому від клієнта на ризики, тобто, чим більший ризик викрадення, тим більший потрібен захист.

2. Оцінювати на рівень захищенності від зловмисного проникнення кожен гаджет, що є в користуванні адвоката чи адвокатської фірми, аналізувати їх на відповідність вимогам безпеки.

3. Використовувати надійні засоби електронного захисту. Надійність може варіюватися від фактів кожного випадку та може включати процедури безпеки, такі як використання безпечного Wi-Fi, браузерів та антишпигунського/антивірусного програмного забезпечення та шифрування.

4. Варто обговорювати із клієнтом відповідний рівень безпеки під час електронного спілкування. Потрібно враховувати рівень обізнаності клієнта з електронними комунікаціями. Якщо клієнт не досвідчений або має обмежений доступ до відповідних технологічних засобів захисту, альтернативний неелектронний зв'язок може стати ефективним засобом для комунікації.

5. Проводити інструктажі для помічників адвоката та інших співробітників технологіям та інформаційній безпеці. Згідно з Типовими правилами 5.1 і 5.3, вжити заходів для того, щоб юристи та допоміжний персонал фірми розуміли, як використовувати безпечні методи спілкування з клієнтами. Також контролювати персонал юридичної фірми, на дотримання процедур безпеки та періодично переглядати та оновлювати процедури безпеки.

6. Обирати надійних осіб/компаній, які надають інформаційно-комунікаційні послуги. Наприклад, при підключенні до мережі Інтернет, чи штатна особа на посаді IT-спеціаліста фірми.

Провівши детальний аналіз Висновку 477R, варто зазначати, що дотримуючись всіх вищезаначених рекомендації адвокат здатний протистояти кіберзагрозам, адже, такий комплексний підхід до захисту відомостей, що становлять авдокатську таємницю убезпечує адвоката та його клієтів від витоку важливих даних. Такий міжнародний досвід, без сумніву, буде корисний для української правової спільноти на шляху до розбудови правової держави.

Ми пропонуємо впровадити комплексні заходи для запобігання розголошенню конфіденційної інформації адвоката та під час надання правничої допомоги. Наші рекомендації охоплюють як технічні, так і організаційні аспекти, що дозволить забезпечити всебічний захист інформації.

Перш за все, слід забезпечити надійний захист електронних інформаційних систем, використовуючи сучасні методи шифрування даних та багатофакторну аутентифікацію для доступу до конфіденційної інформації. Важливо також регулярно оновлювати програмне забезпечення та встановлювати антивірусні програми для захисту від кіберзагроз.

Організаційні заходи повинні включати розробку та впровадження політик конфіденційності, які регламентують порядок обробки та зберігання конфіденційної інформації. Необхідно проводити регулярні тренінги для персоналу, щоб підвищити їх обізнаність щодо важливості захисту інформації та навчити їх правильним методам роботи з конфіденційними даними. Крім того, слід забезпечити фізичний захист документів, зокрема, використовувати сейфи та інші засоби для зберігання паперових носіїв інформації. Важливо також обмежити доступ до конфіденційної інформації лише тим співробітникам, які безпосередньо працюють з нею, та вести облік доступу до таких даних.

З метою мінімізації ризиків витоку інформації під час надання правничої допомоги, адвокатам слід дотримуватися принципу мінімізації даних, тобто збирати та обробляти лише ту інформацію, яка є необхідною для виконання конкретного завдання. Також варто використовувати захищені канали зв'язку для обміну конфіденційною інформацією з клієнтами та іншими сторонами, наприклад, зашифровані електронні поштові сервіси або спеціалізовані платформи для обміну документами. Додатково, важливо впровадити систему моніторингу та аудиту доступу до конфіденційної інформації. Це дозволить вчасно виявляти та реагувати на потенційні загрози. Регулярні перевірки та аудит інформаційних систем допоможуть виявити слабкі місця в системі безпеки та вжити необхідних заходів для їх усунення.

Не менш важливим є впровадження культури безпеки в організації. Це включає створення середовища, де кожен співробітник розуміє свою роль у захисті конфіденційної інформації та дотримується встановлених правил і процедур. Керівництво повинно активно підтримувати та заохочувати дотримання політик безпеки, а також забезпечувати необхідні ресурси для їх реалізації. Також варто розглянути можливість страхування від кіберризиків. Це може допомогти зменшити фінансові втрати у випадку витоку інформації та забезпечити додатковий рівень захисту для адвокатської діяльності. Впровадження цих заходів допоможе значно підвищити рівень захисту конфіденційної інформації в адвокатській діяльності та забезпечити надійний захист прав та інтересів клієнтів.

Висновок. Інформаційна безпека адвоката є однією з найважливіших складових його професійної діяльності,

адже вона забезпечує збереження конфіденційності інформації, захист персональних даних клієнтів, а також дотримання основоположних принципів адвокатської етики. Сучасні реалії цифрової епохи ставлять перед адвокатами нові виклики: зростання кількості кібератак, витоки інформації, фішингові атаки, проникнення шкідливого програмного забезпечення та недоліки в управлінні інформацією. Усе це створює ризики, які можуть суттєво вплинути як на репутацію адвоката, так і на ефективність його роботи.

Проведене дослідження дозволяє зробити висновок, що забезпечення інформаційної безпеки повинно бути пріоритетом для адвокатів на всіх етапах їхньої професійної діяльності. Насамперед це стосується використання сучасних технологій і дотримання відповідних стандартів кібербезпеки. Зокрема, адвокати повинні забезпечувати належний рівень захисту своїх пристроїв, використовуючи антивірусні програми, міжмережеві екрани, системи двофакторної автентифікації та інші засоби захисту даних.

Не менш важливим аспектом є впровадження безпечних каналів комунікації для передачі інформації клієнтам та отримання від них необхідних даних. Шифрування електронної пошти, використання захищених платформ для обміну файлами, а також уникнення незахищених публічних мереж – це мінімальні заходи, яких повинні дотримуватися адвокати для забезпечення конфіденційності.

Окремо варто звернути увагу на регулярне підвищення рівня цифрової грамотності адвокатів. Знання про сучасні кіберзагрози, уміння ідентифікувати потенційно небезпечні дії та адаптація до новітніх технологій дозволять мінімізувати ризики та швидко реагувати на можливі інциденти. Це потребує впровадження регулярних тренінгів, семінарів та консультацій у сфері інформаційної безпеки як для адвокатів, так і для їхнього персоналу.

Також важливим є створення нормативно-правової бази, яка забезпечувала б адвокатів чіткими інструкціями щодо захисту інформації. На рівні адвокатського самоврядування повинні бути розроблені рекомендації чи стандарти інформаційної безпеки, які враховуватимуть специфіку адвокатської діяльності та сучасні виклики.

Особливу увагу слід приділяти технічним рішенням, які дозволяють мінімізувати людський фактор. Автоматизація процесів зберігання та передачі інформації, регулярне резервне копіювання даних, налаштування систем моніторингу кіберзагроз є невід'ємними складовими ефективної системи інформаційної безпеки.

Результати дослідження також демонструють, що без належного рівня інформаційної безпеки адвокат не тільки піддає ризику клієнтську інформацію, але й порушує адвокатську таємницю, що є прямим порушенням етичних норм та чинного законодавства. Зокрема, витік конфіденційної інформації може призвести до значних репутаційних втрат, фінансових санкцій та навіть позбавлення права на здійснення адвокатської діяльності.

Отже, інформаційна безпека адвоката є не просто технічним завданням, а комплексною проблемою, яка вимагає стратегічного підходу, постійного вдосконалення та інтеграції сучасних технологій. Її забезпечення сприяє зміцненню довіри до правничої професії, захисту прав клієнтів, а також підтриманню стабільності в правовій системі загалом.

Забезпечення інформаційної безпеки повинно стати пріоритетом як для окремих адвокатів, так і для всієї системи адвокатського самоврядування. Лише комплексний підхід, що поєднує технічні, організаційні та освітні заходи, здатен створити надійну основу для захисту інформації в умовах сучасного цифрового світу.

ЛІТЕРАТУРА

1. Про адвокатуру та адвокатську діяльність : Закон України № *Відомості Верховної Ради* (ВВР), 2013. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text (дата звернення: 04.11.2024).

2. Про основні засади забезпечення кібербезпеки України : Закон України № (ВВР), 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.11.2024).

3. Діордіца І. В. Кібербезпека адвокатської діяльності в україні та світі. *Нове українське право*. 2021. № 5. С. 105–109.

4. 4.Резнікова Г. І. Інформаційна безпека адвокатської діяльності: криміналістичний погляд. *Науковий вісник Міжнародного гуманітарного університету.* 2017. Т. 2, № 29. С. 120.

5. Колдов, Є. *Адвокат*ська таємниця: дискусійні питання у регулюванні країн Європейського Союзу та України. *Молодий вчений*, 2018. № 11 (63), 847–850.

6. В 2021 році відбувся 391 обшук адвокатів, понад половина – у Київській області й Києві. НААУ. URL: https://unba.org.ua/news/7201-v-2021-roci-vidbuvsya-391-obshuk-advokativ-ponad-polovina-u-kiivs-kij-oblasti-j-kievi.html (дата звернення: 04.11.2024).

7. Дозвіл судді на вилучення смартфону адвоката може містити ознаки злочину – думка. НААУ. URL: https://unba.org.ua/news/8125-dozvil-suddi-na-viluchennya-smartfonu-advokata-mozhe-mistiti-oznaki-zlochinu-dumka.html (дата звернення: 04.11.2024).

8. Національна Асоціація *Адвокат*ів України. Практика ЄСПЛ в контексті обшуків у адвокатів. НААУ. URL: https://unba.org.ua/publications/print/1730-praktika-espl-v-konteksti-obshukiv-u-advokativ.html(дата звернення: 04.11.2024).

9. Завадський, А. А. Інформаційна та кібербезпека адвокатської діяльності: теоретичні та практичні аспекти (досвід США). *Порівняльно-аналітичне право*. № 1. 2020. С. 322.

10. ABA Formal Opinion 477R: Securing communication of protected client information. URL: https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/.(дата звернення: 06.11.2024).