HSA | HIGHER SCHOOL OF ADVOCACY

ЮРИДИЧНА ПРАКТИКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

КИЇВ-2025. ВИЩА ШКОЛА АДВОКАТУРИ

HSA | HIGHER SCHOOL OF ADVOCACY

МИКИТА ФІЛІМОНОВ

адвокат, член ради Комітету НААУ з питань електронного судочинства та кібербезпеки адвокатської діяльності

ТЕТЯНА РАБКО

адвокат, заступник голови Комітету НААУ з питань електронного судочинства та кібербезпеки адвокатської діяльності

ЗМІСТ

ВСТУП

Чому цифрова гігієна важлива для адвоката?

Цифрова гігієна – це сукупність заходів, спрямованих на захист інформації, комунікацій і професійної діяльності адвоката від кіберзагроз, що є критично важливим у контексті цифровізації судочинства в Україні. Відповідно до статті 22 Закону України "Про адвокатуру та адвокатську діяльність", адвокатська таємниця охоплює всю інформацію, отриману від клієнтів, включаючи документи, листування, консультації та відомості про клієнтів. Порушення адвокатської таємниці може призвести до втрати довіри клієнтів, репутаційних збитків, судових позовів або дисциплінарної відповідальності, передбаченої статтею 34 Закону.

Згідно зі звітом IBM Security 2023, середня вартість витоку даних становить $4,45 млн.

При цьому слід врахувати, що в юридичній сфері ця цифра може бути вищою через чутливість інформації. Адвокати, які працюють із контрактами, фінансовими даними, судовими документами та персональними даними клієнтів, є привабливою мішенню для кіберзлочинців.

Наприклад, у 2020 році атака на юридичну фірму Grubman Shire Meiselas & Sacks призвела до викрадення 756 ГБ даних, включаючи контракти знаменитостей.

У контексті України, де активно впроваджується Єдина судова інформаційно-комунікаційна система (ЄСІКС) та електронний документообіг, ризики зростають через використання цифрових платформ, таких як електронний кабінет, Дія.Підпис і автоматизована система виконавчого провадження (АСВП).

Цифрова гігієна допомагає адвокатам та необхідна для забезпечення виконання вимог Закону України "Про захист персональних даних" та GDPR (для роботи з клієнтами з ЄС), а також забезпечує безпечне використання цифрових інструментів, таких як ЄСІКС.

Основні загрози цифровій безпеці адвоката

1. *Втручання в адвокатську таємницю:* Хакери можуть отримати доступ до листування, документів чи баз даних через слабкі паролі, незахищені мережі, зловмисне ПЗ або фізичний доступ до пристроїв. Наприклад, застарілі версії програм, таких як Microsoft Office, часто стають вразливими до атак.

2. *Фішинг:* Шахраї надсилають підроблені листи чи повідомлення, видаючи себе за судові органи, виконавчу службу, клієнтів або банки, щоб отримати доступ до паролів, фінансових даних чи систем. За даними APWG Phishing Activity Trends Report 2023, 94% фішингових атак надходять через електронну пошту.

3. *Шпигунське ПЗ (Spyware):* Програми, які таємно записують дії користувача, перехоплюють листування чи крадуть файли, можуть бути встановлені через шкідливі вкладення, посилання або USB-пристрої.

4. *Витоки конфіденційних даних:* Неправильне зберігання документів у незашифрованих хмарних сховищах, втрата фізичних носіїв або використання незахищених пристроїв може призвести до компрометації інформації. Наприклад, у 2022 році витік даних із хмарного сховища юридичної фірми в США скомпрометував дані 200 000 клієнтів.

5. *Соціальна інженерія:* Зловмисники використовують психологічні маніпуляції, наприклад, дзвінки від "судової адміністрації" чи підроблені листи від колег, щоб отримати доступ до даних.

6. *Атаки на IoT-пристрої:* Розумні пристрої, такі як камери, принтери чи сканери в офісі, можуть бути вразливими до атак, якщо не захищені належним чином.

7. *Компрометація електронних кабінетів:* Через використання слабких паролів або незахищених підключень до ЄСІКС чи АСВП зловмисники можуть отримати доступ до документів, судових рішень чи персональних даних сторін.

Мета посібника

Цей посібник розроблено для надання адвокатам практичних рекомендацій з цифрової гігієни, адаптованих до сучасних викликів цифровізації судового процесу та виконавчого провадження в Україні. Він охоплює захист даних, безпечне використання ЄСІКС, управління паролями, захист комунікацій, протидію фішингу, соціальну інженерію, аудит безпеки та рекомендації щодо роботи з електронними виконавчими документами. Посібник враховує реалії сьогодення та сучасні кіберзагрози, надаючи чіткі інструкції для впровадження.

БАЗОВІ ПРИНЦИПИ ЦИФРОВОЇ БЕЗПЕКИ

Оновлення та патчі безпеки

Регулярне оновлення операційних систем (Windows, macOS, Linux) і програмного забезпечення є основою цифрової безпеки. За даними Cybersecurity and Infrastructure Security Agency (CISA), 60% кібератак використовують відомі вразливості, для яких уже доступні патчі. У контексті адвокатської діяльності, де використовуються платформи, такі як ЄСІКС, оновлення спеціалізованого ПЗ є критично важливим для захисту документів клієнтів.

Рекомендації:

• Увімкніть автоматичне оновлення для ОС, браузерів (Chrome, Firefox), Microsoft Office, Adobe Acrobat.

• Налаштуйте сповіщення про оновлення для спеціалізованого ПЗ, яке не оновлюється автоматично.

• Щомісяця перевіряйте та встановлюйте патчі безпеки для всіх пристроїв.

• Для Linux-систем використовуйте команди, такі як sudo apt update && sudo apt upgrade (Ubuntu) або sudo dnf update (Fedora), для підтримки актуальності.

• Уникайте використання застарілих ОС (наприклад, Windows 7), які не отримують оновлення безпеки.

• Регулярно перевіряйте оновлення для клієнтських додатків, щоб уникнути вразливостей.

Принцип мінімізації ризиків

Мінімізація ризиків передбачає зменшення вразливих точок у цифровій інфраструктурі адвоката. Наприклад, використання одного пароля для доступу до електронної пошти та електронного підпису значно підвищує ризик компрометації. За даними Verizon Data Breach Report 2023, 80% витоків даних пов'язані зі слабкими або повторно використаними паролями.

Рекомендації:

• Створюйте унікальні паролі для кожного сервісу (електронна пошта, електронний підпис, хмарні сховища).

• Не зберігайте чутливі документи (документи клієнтів, процесуальні документи, судові рішення, виконавчі документи) у незашифрованому вигляді на комп'ютері чи в хмарі.

• Уникайте використання публічних комп'ютерів для доступу до ЄСІКС чи інших юридичних платформ.

• Регулярно перевіряйте дозволи доступу до файлів і папок на комп'ютері, особливо в мережевих папках, що використовуються для обміну документами.

Двофакторна аутентифікація (2FA)

Двофакторна аутентифікація додає додатковий рівень захисту, вимагаючи другий фактор підтвердження (код із додатка, апаратний ключ або біометричні дані) під час входу. За даними Microsoft, 2FA значно знижує ризик компрометації. SMS-коди є менш безпечними через можливість SIM-спуфінгу, тому перевагу слід надавати апаратним ключам або додаткам-аутентифікаторам.

Рекомендації:

• Використовуйте апаратні ключі безпеки, такі як YubiKey або Nitrokey, для доступу до ЄСІКС та поштових сервісів.

• Встановіть додатки-аутентифікатори (Google Authenticator, Authy, Microsoft Authenticator) для генерації одноразових кодів.

• Уникайте SMS-кодів для 2FA, особливо для критичних сервісів.

• Зберігайте резервні коди доступу в зашифрованому менеджері паролів.

• Увімкніть 2FA для всіх сервісів, включаючи Google Workspace, Microsoft 365, Dropbox.

Розмежування особистого та професійного простору

Використання особистих пристроїв або акаунтів для роботи підвищує ризик витоку даних. Компрометація особистого телефону може відкрити доступ до робочих документів.

Рекомендації:

• Використовуйте окремий ноутбук і смартфон для роботи з юридичними платформами.

• Створіть окремі електронні адреси для професійного листування (наприклад, advokat@gmail.com) та особистих справ.

• Уникайте використання особистих соціальних мереж для контактів із клієнтами чи для вирішення робочих питань.

• Налаштуйте окремі профілі користувачів на комп'ютері для роботи та особистих потреб.

ЗАХИСТ ОБЛАДНАННЯ ТА ОПЕРАЦІЙНИХ СИСТЕМ

Безпека смартфонів і ноутбуків

Використання шифрування

Шифрування захищає дані на пристрої у разі втрати чи крадіжки. Без шифрування зловмисники можуть отримати доступ до процесуальних документів, електронних судових рішень із ЄСІКС чи клієнтських даних.

Рекомендації:

• На Windows увімкніть BitLocker (доступно у Windows 10/11 Pro) для шифрування дисків. Зберігайте ключ відновлення в безпечному місці.

• На macOS активуйте FileVault у системних налаштуваннях для повного шифрування диска.

• Використовуйте VeraCrypt для створення зашифрованих контейнерів для судових документів.

• На Android увімкніть шифрування в налаштуваннях безпеки (за замовчуванням у сучасних версіях).

• На iOS шифрування вбудовано, але використовуйте складний пароль і біометричний захист.

Захист SIM-карт

Одна з небезпечних злочинних махінацій – перевипуск sim-картки без відома власника. Отримавши контроль над вашим номером, зловмисники можуть зламати електронні облікові записи та використати їх для зловмисних цілей.

Рекомендації:

• Увімкніть заборону переадресації дзвінків і SMS у оператора зв’язку (Vodafone, Київстар, Lifecell).

• Встановіть PIN-код для SIM-карти в налаштуваннях телефону.

• Використовуйте eSIM, яка складніша для клонування.

• Перевіряйте активність номера через особистий кабінет оператора.

Вимкнення Bluetooth та Wi-Fi у громадських місцях

Bluetooth і Wi-Fi можуть бути використані для атак, таких як BlueBorne, що дозволяють отримати доступ до пристрою.

Рекомендації:

• Вимикайте Bluetooth і Wi-Fi у громадських місцях (аеропорти, суди, кафе, готелі).

• Використовуйте фізичні перемикачі для відключення бездротових модулів на ноутбуках.

• Увімкніть режим польоту на смартфоні, коли бездротовий зв’язок не потрібен.

• Налаштуйте автоматичне відключення Wi-Fi, якщо пристрій не підключений до відомої мережі.

Захист від фізичного доступу

Фізичний доступ до пристрою може призвести до компрометації документів чи даних клієнтів.

Рекомендації:

• Встановіть складний пароль (не менше 12 символів) і увімкніть біометричний контроль.

• Налаштуйте віддалене блокування та стирання даних через Find My Device (Android) або Локатор (Apple).

• Використовуйте захисні екрани (privacy screens) для ноутбуків у судах чи громадських місцях.

• Не залишайте пристрої без нагляду в офісі чи судах. Використовуйте замки Kensington.

Безпека USB-накопичувачів та зовнішніх пристроїв

Неперевірені USB-накопичувачі можуть містити шкідливе ПЗ, наприклад, BadUSB, яке імітує клавіатуру для виконання команд.

Рекомендації:

• Використовуйте лише перевірені USB-накопичувачі. Уникайте флешок із конференцій чи від незнайомих осіб.

• Зашифруйте дані на флешках за допомогою VeraCrypt або BitLocker To Go.

• Вимкніть автозапуск зовнішніх пристроїв у налаштуваннях ОС.

• Використовуйте USB-порти з функцією лише зарядки для невідомих пристроїв.

ПАРОЛЬНИЙ МЕНЕДЖМЕНТ ТА ДОСТУП ДО ЄСІКС

Принципи створення надійних паролів

Надійний пароль до Вашого електронного підпису є першим бар'єром захисту від несанкціонованого доступу до електронного кабінету ЄСІКС. За даними Forbes Advisor, 46% американців за останній рік стали жертвами зламу паролів. Серед 1,8 млн зламаних паролів найчастішими були: admin, 123456, password і подібні.

Рекомендації:

- Пароль має бути не коротшим за 8-12 символів, із комбінацією літер верхнього та нижнього регістру, цифр і спеціальних символів (наприклад, K9#mP2$kL7@qW3&zX8).
- Використовуйте фрази-паролі, наприклад, "Судовий3бір2025!ЄСІКС ".
- Уникайте особистих даних (імена, дати народження).
- Генеруйте паролі за допомогою менеджерів паролів або функцій.
- Регулярно змінюйте паролі.

Менеджери паролів

Зберігання паролів у браузері є небезпечним через вразливості, які можуть скомпрометувати доступ до юридичних платформ.

Рекомендації:

• Використовуйте менеджери паролів: Bitwarden, 1Password, KeePassXC.

• Налаштуйте головний пароль для менеджера (не менше 20 символів).

• Експортуйте базу паролів у зашифрованому вигляді та зберігайте на зашифрованому носії.

• Увімкніть автозаповнення лише для перевірених пристроїв.

Політика зміни паролів

Часта зміна паролів без необхідності може призвести до використання слабших паролів.

Рекомендації:

• Міняйте паролі після підозри на компрометацію або раз на 6–12 місяців.

• Використовуйте менеджер паролів для генерування нових паролів.

• Перевіряйте паролі на витоки через Have I Been Pwned.

• Налаштуйте сповіщення про витоки даних через Firefox Monitor.

БЕЗПЕКА КОМУНІКАЦІЙ ТА ДОКУМЕНТООБІГУ

Месенджери з наскрізним шифруванням

Популярні месенджери (Viber, WhatsApp) не забезпечують достатнього захисту для збереження конфіденційної інформації під час здійснення адвокатської діяльності.

Рекомендації:

• Використовуйте Signal із наскрізним шифруванням і функцією самознищення повідомлень.

• Альтернативи: Session (децентралізована, без прив'язки до номера) або Threema (анонімність, платна).

• Перевіряйте номери безпеки контактів для захисту від перехоплення.

• Налаштуйте самознищення повідомлень для чутливих розмов.

• Уникайте Telegram для конфіденційних переговорів.

Електронна пошта

Звичайні поштові сервіси не забезпечують наскрізного шифрування для забезпечення повної конфіденційності листування.

Рекомендації:

• Використовуйте ProtonMail або Tutanota для зашифрованого листування.

• Налаштуйте PGP/GPG для підпису та шифрування листів (Thunderbird + Enigmail, Gpg4win).

• Створюйте зашифровані архіви з паролем для надсилання документів.

• Перевіряйте налаштування безпеки поштового клієнта (TLS/SSL).

• Використовуйте унікальні email-адреси для різних клієнтів чи проєктів.

Передача файлів

Незашифровані хмарні сховища (Google Drive, Dropbox) вразливі до витоків даних.

Рекомендації:

• Використовуйте Tresorit або Sync.com для зашифрованого зберігання документів.

• Для одноразової передачі використовуйте OnionShare (через Tor) або Cryptomator.

• Створюйте зашифровані ZIP-архіви перед надсиланням файлів.

• Перевіряйте одержувача через захищені канали (Signal).

• Уникайте USB-флешок для передачі судових документів.

Робота з електронним кабінетом ЄСІКС

Електронний кабінет ЄСІКС є ключовим інструментом для обміну процесуальними документами між учасниками справи та судом, отримання судових рішень і виконавчих документів.

Рекомендації:

• Використовуйте Дія.Підпис або апаратні ключі (YubiKey) для входу в ЄСІКС .

• Перевіряйте сповіщення про доставку документів у електронний кабінет.

• Зберігайте отримані документи в зашифрованому вигляді (VeraCrypt).

• Уникайте доступу до ЄСІКС через громадські Wi-Fi без VPN.

• Регулярно перевіряйте логи активності в електронному кабінеті на підозрілі входи.

ЗАХИСТ ВІД КІБЕРАТАК ТА ФІШИНГУ

Розпізнавання фішингових атак

Фішинг часто імітує листи від судів, виконавчої служби чи клієнтів.

Рекомендації:

• Перевіряйте домен відправника (наприклад, court.gov.ua, а не court-gov-ua.com).

• Уникайте переходу за посиланнями в листах; відкривайте ЄСІКС вручну.

• Звертайте увагу на орфографічні помилки чи термінові заклики до дії.

• Використовуйте плагіни uBlock Origin або HTTPS Everywhere для блокування шкідливих сайтів.

• Пройдіть тренінг із розпізнавання фішингу.

Захист від зловмисного ПЗ

Шкідливе ПЗ може бути встановлено через вкладення чи посилання в листах, що імітують ЄСІКС.

Рекомендації:

• Встановіть надійний антивірус.

• Налаштуйте брандмауер для блокування підозрілих додатків.

• Уникайте завантаження файлів із неперевірених джерел.

• Скануйте пристрій після роботи з невідомими файлами.

• Використовуйте Windows Sandbox для тестування файлів.

Безпека у громадських Wi-Fi-мережах

Громадські Wi-Fi у судах чи кафе вразливі до атак "людина посередині".

Рекомендації:

•Використовуйте VPN (ProtonVPN, IVPN).

• Вимкніть автоматичне підключення до Wi-Fi.

• Перевіряйте HTTPS-підключення в браузері.

• Налаштуйте DNS через Cloudflare (1.1.1.1) або Quad9.

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ОСОБИСТА БЕЗПЕКА

Маніпулятивні методи

Соціальна інженерія може імітувати дзвінки від "судової адміністрації" чи "виконавчої служби".

Рекомендації:

• Не надавайте паролі чи PIN-коди по телефону чи через email.

• Перевіряйте запити через захищені канали.

• Пройдіть тренінги з кібербезпеки.

• Верифікуйте особу відправника через відомий номер.

Захист у соціальних мережах

Соціальні мережі можуть бути джерелом інформації для зловмисників.

Рекомендації:

• Обмежте видимість особистих даних у Facebook, LinkedIn, Instagram.

• Використовуйте псевдоніми для особистих акаунтів.

• Увімкніть сповіщення про спроби входу.

• Видаляйте підозрілі програми, підключені до акаунтів.

• Уникайте публікації конфіденційної інформації про судові справи чи виконавче провадження.

Шахрайство з електронними підписами

Підроблені підписи можуть використовуватися для фальсифікації документів.

Рекомендації:

• Перевіряйте підписи через Дія.Підпис, Adobe Acrobat або DocuSign.

• Використовуйте апаратні токени (YubiKey, Nitrokey) для підписів.

• Зберігайте ключі підпису в зашифрованому вигляді.

• Навчайте клієнтів перевіряти справжність підписів.

БЕЗПЕЧНА РОБОТА З ДОКУМЕНТАМИ В ЄСІКС

Отримання та обробка документів у ЄСІКС

Електронний кабінет ЄСІКС дозволяє отримувати судові рішення та виконавчі документи.

Рекомендації:

- Використовуйте Дія.Підпис або апаратні ключі для автентифікації.
- Перевіряйте сповіщення про доставку документів у кабінет.
- Зберігайте документи в зашифрованих контейнерах (VeraCrypt).
- Уникайте завантаження документів на незахищені пристрої.
- Перевіряйте логи активності в ЄСІКС на підозрілі дії.

Важливо! Документи, підписані кваліфікованим електронним підписом (в т.ч. декількома підписами) допускається завантажувати до підсистеми «Електронний суд» у форматі zip-архіву як додаток до процесуальних документів.

Для створення документу з декількома КЕП необхідно обрати формат підписання документу CAdES. Дані та підпис зберігаються в CMS файлі (*.p7s)

Підписуємо файл (наприклад, 123.pdf) першим електронним підписом. Завантажуємо підписаний файл (буде 123.pdf.p7s).

Підписуємо цей файл 123.pdf.p7s другим електронним підписом. Завантажуємо підписане (буде 123.pdf.p7s.p7s).

Таким чином маємо 123.pdf.p7s.p7s — це й буде файл, підписаний двома підписами.

Протокол створення та перевірки кваліфікованого та удосконаленого електронного підпису містить наступні реквізити:

- ✓ Прізвище ім'я по батькові особи, що наклала електронний підпис (для юридичних осіб додатково зазначається назва організації та код ЄДРПОУ);
- ✓ Дату та час підпису;
- ✓ РНОКПП підписувача;
- ✓ Інформацію про те ким видано Сертифікат;
- ✓ Серійний номер електронного підпису.

Подання виконавчих документів

Стягувачі можуть подавати електронні виконавчі документи онлайн за допомогою функціоналу ЄСІКС

Рекомендації:

- Використовуйте захищені канали для подання документів (HTTPS, VPN).
- Перевіряйте правильність заповнення форм у ЄСІКС .

• Зберігайте підтвердження подання в зашифрованому вигляді.

• Уникайте листування з державними чи приватним виконавцем через незахищені email.

Сплата судового збору та штрафів онлайн

Боржники можуть сплачувати судовий збір через ЄСІКС або Портал Дія.

Рекомендації:

• Використовуйте захищені платіжні системи (Портал Дія, LiqPay).

• Перевіряйте реквізити платежу перед відправкою.

• Зберігайте квитанції про сплату в зашифрованому вигляді.

• Уникайте використання громадських Wi-Fi для платежів.

КОНТРОЛЬ ЦИФРОВОЇ БЕЗПЕКИ ТА АУДИТ

Перевірка витоків даних

Сервіси, такі як Have I Been Pwned, допомагають виявити компрометацію email чи паролів.

Рекомендації:

- Перевіряйте email-адреси через Have I Been Pwned або Firefox Monitor.
- Змінюйте паролі та увімкніть 2FA у разі витоку.
- Налаштуйте сповіщення про нові витоки.

Резервне копіювання

Метод 3-2-1: три копії даних, на двох різних пристроях, одна офлайн.

Рекомендації:

- Використовуйте зашифровані жорсткі диски для офлайн-копій (VeraCrypt).
- Для хмарного копіювання обирайте Tresorit або Sync.com.
- Тестуйте відновлення даних із копій.
- Зберігайте офлайн-копії в сейфі.
- Автоматизуйте копіювання через Duplicati або Restic.

Щомісячний аудит

Регулярний аудит виявляє слабкі місця в безпеці.

Рекомендації:

- Видаляйте непотрібні акаунти через JustDeleteMe.
- Перевіряйте дозволи доступу до ЄСІКС, Google Drive, Dropbox.
- Аналізуйте логи активності в ЄСІКС і поштових сервісах.
- Використовуйте Google Account Activity або Microsoft Account Security.
- Видаляйте застарілу інформацію через запити до адміністраторів сайтів.

ВИСНОВОК ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

12 головних правил цифрової гігієни

1. Оновлюйте ОС та програми.
2. Використовуйте унікальні паролі та менеджер паролів.
3. Увімкніть 2FA для роботи з електронними сервісами.
4. Розмежуйте особисті та професійні пристрої й акаунти.
5. Шифруйте дані на пристроях і в хмарах.
6. Використовуйте Signal для конфіденційних розмов.
7. Застосовуйте VPN у громадських мережах.
8. Навчіться розпізнавати фішинг і соціальну інженерію.
9. Обмежте публічну інформацію в соціальних мережах.
10. Перевіряйте електронні підписи через Дія.Підпис.
11. Зберігайте важливі документи в зашифрованому вигляді.
12. Проводьте щомісячний аудит і резервне копіювання.

Чек-лист для самоперевірки

- Усі пристрої оновлені.
- 2FA увімкнено для роботи з електронними сервісами.
- Використовується менеджер паролів.
- Дані зашифровані (BitLocker, FileVault, VeraCrypt).
- Використовуються Signal і ProtonMail.
- VPN налаштовано для громадських мереж.
- Створено резервні копії за методом 3-2-1.
- Перевірено витоки через Have I Been Pwned.
- Видалено непотрібні акаунти.
- Перевірено підписи через Дія.Підпис.

Додаткові ресурси:

- Have I Been Pwned: https://haveibeenpwned.com
- ProtonMail: https://proton.me
- Signal: https://signal.org
- Bitwarden: https://bitwarden.com

- Tresorit: https://tresorit.com
- JustDeleteMe: https://justdeleteme.xyz
- Gpg4win: https://gpg4win.org
- KnowBe4: https://www.knowbe4.com
- ЄСІКС: https://cabinet.court.gov.ua
- Дія.Підпис: https://diia.gov.ua

HSA | HIGHER SCHOOL OF ADVOCACY

hsa.org.ua

@hsa.org.ua

@hsaorgua