***Левченко Дарина Олександрівна,***
студентка н.гр. 103_СПД ННІ права та психології НАВС

*Науковий керівник:*
***Хахановський Валерій Георгійович***
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

# КІБЕРБЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ У РОБОТІ ЮРИСТА ТА ПСИХОЛОГА: СУЧАСНІ ЗАГРОЗИ ТА ТЕХНОЛОГІЧНІ РІШЕННЯ

У сучасних умовах цифровізації юридичної та психологічної практики питання захисту персональних даних клієнтів набуває пріоритетного значення. У роботі юриста та психолога обробляється інформація, що належить до категорії конфіденційної, а часто — до чутливої (intimate/sensitive data): медичні дані, психологічний стан, результати тестувань, особисті історії, дані кримінального провадження, фінансова інформація, матеріали адвокатської таємниці тощо. Порушення конфіденційності може спричинити юридичну відповідальність, професійну дискваліфікацію, моральну шкоду для клієнта, втрату репутації фахівця.

Водночас збільшення кількості онлайн-консультацій, використання хмарних сервісів, електронних доказів, дистанційних платформ та месенджерів значно підвищує ризики несанкціонованого доступу до інформації. Важливим є впровадження комплексних технічних і організаційних заходів, що забезпечують відповідність законодавству України, загальним стандартам кібербезпеки та міжнародним практикам (GDPR, NIST, ISO/IEC 27001).

*Нормативно-правове підґрунтя захисту персональних даних у юридичній та психологічній практиці:*

Закон України «Про захист персональних даних» (№2297-VI).

Закон визначає:

- поняття персональних даних та їхні категорії;
- обов’язки володільців і розпорядників даних;
- вимоги до згоди суб’єкта;
- принципи обробки: законність, пропорційність, мінімізація, точність, обмеження строків;
- необхідність впровадження організаційних і технічних заходів безпеки.

Для юриста та психолога визначальними є статті щодо чутливих даних, адже інформація клієнтів належить до категорій, які потребують підвищеного захисту.

*Загальний регламент ЄС із захисту даних (GDPR) – як міжнародний орієнтир.*

Хоча Україна формально не підпадає під дію GDPR, його принципи є міжнародним стандартом:

- «privacy by design» та «privacy by default»;
- необхідність Data Protection Impact Assessment (DPIA) при роботі з ризиковими даними;
- право клієнта на стирання, перенесення, доступ;
- вимоги до безпечної передачі даних.

Адвокатська таємниця (Закон України «Про адвокатуру та адвокатську діяльність»)

Юрист зобов'язаний забезпечити конфіденційність:

- матеріалів справи;
- електронних документів;
- листування з клієнтом;
- чернеток та нотаток;
- файлів у смартфоні, ноутбуці та хмарних сховищах.

Порушення конфіденційності є дисциплінарним проступком.

Етичні стандарти психолога

Кодекси етики забороняють розкривати інформацію про клієнта, окрім випадків загрози життю.

Це накладає технологічні зобов'язання:

- безпечне зберігання записів сесій;
- недопущення використання небезпечних месенджерів;
- обмеження доступу сторонніх осіб.

**Сучасні кіберзагрози для юристів і психологів.**

*Фішинг і соціальна інженерія*

Близько 90% кібератак у світі починаються з фішингу. Атакувальники можуть:

- видавати себе за клієнта;
- надсилати «документи справи» або «результати тестів» як заражені файли;
- використовувати месенджери та соціальні мережі;
- підробляти email встановленого домену.

Юристи та психологи – ідеальні цілі, бо працюють із приватною інформацією.

Злам месенджерів і електронної пошти

Більшість випадків витоку конфіденційних даних відбувається через:

- слабкі паролі;
- відсутність двофакторної автентифікації (MFA);
- збереження паролів у браузері;
- синхронізацію на незахищених пристроях.

Витоки через незахищені онлайн-платформи

Небезпеку становлять:

- безкоштовні сервіси відеозв'язку без end-to-end шифрування;
- застарілі або «піратські» програми;
- неперевірені онлайн-тести й додатки для психологів;
- CRM-системи з низьким рівнем захисту.

Атаки на хмарні сховища

Проблеми виникають через:

- неправильно налаштовані права доступу;
- слабкі корпоративні паролі;
- відсутність контролю активності;
- сторонні підключення.

Ransomware (віруси-вимагачі)

Шифрування файлів клієнтів із вимогою викупу стало головною загрозою для приватних кабінетів.

Ризики:

- повна втрата бази клієнтів;
- витік документів справи;
- шантаж;
- кримінальна відповідальність за недбале зберігання персональних даних.

Інсайдерські загрози

До них належать:

- доступ помічників до конфіденційних матеріалів;
- випадкові витоки через копіювання файлів;
- неправильна передача документів у messengers;
- робота з документами у спільних Google-дисках.

**Принципи кіберзахисту для юристів і психологів.**

*Мінімізація даних*

Збирати лише те, що потрібно.

Психологу не потрібно знати адресу клієнта; юристу – сімейний стан, якщо це не має значення для справи.

Розмежування доступу

- кожен співробітник має доступ лише до тих файлів, які потрібні для роботи;
- заборонено передавати дані через особисті акаунти;
- не дозволяти сім'ї або друзям користуватися робочим ноутбуком.

Шифрування

- шифрування диска: BitLocker, FileVault, VeraCrypt;
- шифрування листування: E2EE;
- шифрування архівів із паролем;
- шифрування резервних копій.

MFA/2FA — основа сучасного захисту

Вести професійну діяльність без MFA — критична помилка.

Захист мобільних пристроїв

Оскільки психологи та юристи часто працюють зі смартфона:

- PIN 6+ цифр;

- біометрія;
- вимкнення push-сповіщень для месенджерів, де обговорюються справи;
- заборона автоматичного створення скрінів.

**Технологічні рішення для безпечної практики.**

Безпечні месенджери

Рекомендовані: Signal, Threema, WhatsApp (E2EE).

Умовно дозволені з певними застереженнями:

- Telegram (НЕ E2EE у чатах за замовчуванням, немає E2EE у групах).

Заборонені для конфіденційної роботи:

- Instagram Direct
- Facebook Messenger
- Viber (немає перевірки ключів і слабка реалізація E2EE).

Відеозв'язок для онлайн-консультацій

*Психологам:*

- Google Meet (якщо підключено корпоративний Google Workspace),
- Zoom (лише в корпоративній версії з E2EE),
- VSee (медично орієнтована платформа),
- Doxy.me (для телемедицини).

*Юристам:* Microsoft Teams, Google Meet, Zoom з E2EE.

Не рекомендовано: Telegram-дзвінки, Skype, Facebook Messenger Rooms.

*Хмарні сховища*

Найбезпечніші:

- Google Workspace (корпоративний рівень)
- Microsoft OneDrive for Business
- Tresorit (повне шифрування)
- Proton Drive

Заборонені для конфіденційних даних:

- безкоштовні Google-диски без обмеження доступу;
- iCloud без MFA;
- Dropbox Basic.

*Менеджери паролів.*

Варто використовувати: Bitwarden, 1Password, KeePassXC.

НЕ рекомендується: зберігати паролі у браузері, паролі у нотатках телефону.

Антивірус і захисне ПЗ

Рекомендовані рішення:

- Bitdefender
- Kaspersky (тільки якщо немає законодавчих обмежень)
- ESET
- Microsoft Defender (вбудований, але надійний)

Також важливі: фільтрація вкладень у пошті, блокування небезпечних сайтів, функція виявлення ransomware.

**Організаційні заходи**

*Політика безпеки*

Має містити:

• правила доступу; правила зберігання документів; порядок резервного копіювання; обов'язки співробітників; порядок реагування на інциденти; порядок ведення онлайн-консультацій.

*Навчання персоналу*

Щонайменше раз на рік проводиться навчання щодо: фішингу; використання робочих пристроїв; заборонених сервісів; алгоритму реагування при атаці.

Угоди про нерозголошення (NDA)

Підписуються: з помічниками; адміністраторами; перекладачами; технічним персоналом.

Оцінка впливу DPIA

Проводиться при: використанні нових платформ; обробці чутливих медичних/психологічних даних; перенесенні даних у хмару.

**Рекомендації для психолога.**

Психолог працює з даними: про психічний стан; діагностичні тести; результати терапії; історії травм; записи сесій.

Це особливо чутлива інформація.

Психолог зобов'язаний:

1. Використовувати окремий робочий пристрій.
2. Не проводити консультації через небезпечні месенджери.
3. Заборонити запис екрана у смартфоні.
4. Зберігати записи сесій у зашифрованому вигляді.
5. Обмежувати доступ до календаря з розкладом клієнтів.
6. Використовувати платформи, адаптовані до медичної конфіденційності (VSee, Doxy).

**Рекомендації для юриста.**

Юрист працює з: документами кримінальних проваджень; персональними даними сторін; фінансовими документами; доказами; відео/аудіоматеріалами; матеріалами з обмеженим доступом.

Юристу необхідно:

1. Шифрувати досьє та усі резервні копії.
2. Використовувати електронний підпис тільки через сертифіковані сервіси.
3. Уникати пересилання документів клієнта через месенджери.
4. Створити захищений канал обміну файлами (ProtonDrive, Tresorit).
5. Заборонити ведення справи через особисту пошту (тільки корпоративна).

**План реагування на інциденти**

Алгоритм

У разі підозри на витік:

1. Негайно ізолювати пристрій.
2. Змінити паролі та закрити сесії входів.
3. Перевірити журнали активності у хмарі.

4. Повідомити керівництво або клієнта (залежно від законодавства).
5. Оцінити масштаб витоку.
6. Відновити дані з резервної копії.
7. Оформити інцидент у внутрішньому журналі.

**Висновок.**

Юрист і психолог працюють із вразливими категоріями інформації, тому зобов'язані забезпечити найвищий рівень кіберзахисту. Сучасні загрози – фішинг, соціальна інженерія, ransomware, злом месенджерів, вразливі онлайн-платформи – вимагають комплексного підходу:технічного (шифрування, MFA, безпечні пристрої), організаційного (політики, навчання, NDA) та правового (дотримання Закону України, рекомендацій міжнародних стандартів).

Ефективна стратегія кібербезпеки – це не одноразова дія, а системна робота, яка підвищує захист професіонала та довіру клієнтів.

**Список використаних джерел:**


1. Закон України «Про захист персональних даних» №2297-VI.
2. Закон України «Про адвокатуру та адвокатську діяльність».
3. GDPR — General Data Protection Regulation (Regulation (EU) 2016/679).
4. NIST SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information.
5. ISO/IEC 27001:2022 — Information Security Management Systems.
6. OWASP Top 10 Web Application Security Risks.
7. National Cyber Security Centre (NCSC). Cyber Security Guidance.
8. American Psychological Association (APA). Guidelines for Telepsychology.
9. LawTech Today. Cybersecurity Best Practices for Attorneys.
10. European Federation of Psychologists' Associations. Ethical Guidelines for Online Therapy.