БЕЗПЕЧНІ КОМУНІКАЦІЇ НОТАРІУСА ІЗ ЗАІНТЕРЕСОВАНИМИ ОСОБАМИ, ЩО ЗВЕРТАЮТЬСЯ ДО НЬОГО

Комісія з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності

спікер Олександр СПЕРЧУН

заступник голови комісії

ПЛАН

1. Збереження приватності та конфіденційності під час комунікацій.
2. Застосування принципу «нульової довіри» (Zero Trust) в комунікаціях.
3. Використання цифрових підписів для підтвердження автентичності документів.
4. Використання засобів шифрування для безпеки комунікацій.
5. Безпечна передача інформації.

Чому це важливо?

Сьогодні питання безпечних комунікацій для нотаріусів є критично важливим, оскільки вони постійно працюють із інформацією, що становить, у тому числі, нотаріальну таємницю. Інформація, з якою оперує нотаріус, підлягає особливому захисту, зокрема відповідно до законодавства про захист персональних даних. Зважаючи на цифровий розвиток світу, інформація з обмеженим доступом має безпечно зберігатися та передаватися відповідними способами, що відповідають сучасним вимогам кібербезпеки.

Збереження нотаріальної таємниці та захист персональних даних у комунікаціях нотаріуса є одним із ключових завдань, оскільки будь-яка втрата чи витік інформації може призвести до серйозних правових наслідків як для нотаріуса, так і для осіб, які звертаються до нього.

Для забезпечення збереження нотаріальної таємниці нотаріус має гарантувати, що інформація передається лише особам, які мають на це право, і виключно безпечними каналами зв’язку.

Контроль доступу до інформації є важливим аспектом роботи нотаріуса. Це означає, що доступ до даних мають лише ті, хто отримав на це дозвіл, і тільки в обсязі, потрібному для виконання їхніх завдань. Наприклад, коли нотаріус взаємодіє з іншими особами в інтересах особи, яка звернулася до нього, важливо передавати лише мінімально необхідну інформацію, щоб уникнути розголошення персональних даних осіб та конфіденційної інфомації. Такий підхід допомагає захистити дані від витоків і зберігати їх у безпеці.

Отже, для нотаріусів безпечні комунікації означають не лише захист від зовнішніх загроз, але й забезпечення високого рівня внутрішнього контролю за дотриманням стандартів конфіденційності, санкціонованого доступу та захисту персональних даних осіб, які звертаються до них.

Збереження приватності та конфіденційності під час комунікацій

- Використовуйте месенджери з наскрізним шифруванням (наприклад, Signal, WhatsApp).
- Не діліться конфіденційною інформацією через незахищені додатки, особливо у відкритих або сумнівних каналах та соціальних мережах.
- Будьте обережні з телефонними дзвінками та електронним листуванням, не обговорюйте та не передавайте конфіденційну інформацію без встановлення та підтвердження особи запитувача і обсягу повноважень.
- Перевіряйте дзвінок, якщо невідома особа просить вас надати номер банківської карти, паролі, пін коди тощо.
- Будьте обережні при очному спілкуванні, пам'ятайте, що розмова може бути записана співрозмовником без вашого відома.
- Уникайте обговорення конфіденційних питань по телефону, або в публічних місцях, пам’ятайте розмову можуть прослухати.

Застосування принципу «нульової довіри» (Zero Trust) в комунікаціях

Суть принципу в тому, що в будь-якій взаємодії не можна автоматично довіряти жодному контакту, користувачеві або пристрою. Кожен запит на доступ до інформації або ресурсів має проходити перевірку, незалежно від джерела.

Приклад застосування Zero Trust у комунікаціях нотаріуса та нотаріальній діяльності:

- При отриманні будь-яких повідомлень або запитів на інформацію не поспішайте відповідати. Спершу дайте собі відповідь на такі запитання: чи знайомий вам контакт? чи очікуєте ви цей запит? чи можна надавати запитувану інформацію? чи використовується звичний для вас і контакту спосіб комунікації? чи можете ви додатково ідентифікувати контакт, окрім імені?
- Завжди підтверджуйте особу запитувача перед обміном інформацією, навіть якщо ця особа здається вам знайомою. Особливо це важливо для комунікацій у текстовій або електронній формі.
- Обмежуйте обмін даними до конкретної інформації, якою особа має право володіти. Це дозволяє мінімізувати ризик витоку зайвої інформації.
- Рекомендуйте вашим контактам використовувати захищені методи комунікації.

Використання цифрових підписів для підтвердження автентичності документів

Цифровий підпис дозволяє підтвердити, що документ не був змінений після підписання, а також що він справді походить від зазначеного підписанта. Це критичний елемент безпеки електронних документів, що забезпечує юридичну чинність.

Застосування у роботі нотаріуса:

- Використовуйте цифровий підпис для усіх документів, які передаються електронним шляхом, щоб отримувачі були впевнені у їх автентичності.
- За можливості, підписуйте цифровим підписом не лише основні документи, але й важливі повідомлення, що містять вимоги, запити, звітність, офіційне листування тощо.
- Розкажіть своїм контактам про переваги використання цифрових підписів, поясніть, як це забезпечує цілісність і конфіденційність документів.

Використання засобів шифрування для безпеки комунікацій

Шифрування — це процес кодування інформації з метою запобігання несанкціонованого доступу. У разі викрадення або витоку, зашифровані дані будуть недоступні для прочитання без відповідного ключа.

Наступні заходи забезпечать комплексний захист конфіденційних даних нотаріуса, допоможуть зберегти приватність і мінімізують ризик витоків інформації в електронній комунікації:

- **Використовуйте захищені месенджери з наскрізним шифруванням, щоб захистити повідомлення від стороннього доступу.**
- **Шифруйте файли із важливою інформацією перед відправкою.**
- **Використовуйте шифрування жорсткого диска, щоб у разі втрати, крадіжки або вилучення пристрою ваші дані залишалися захищеними.**
- **Використовуйте VPN із шифруваннями для захищеного підключення до неперевірених мереж.**
- **Зберігайте всі резервні копії важливих документів у зашифрованому вигляді, щоб у разі втрати доступу конфіденційність залишалася захищеною.**
- **Для перенесення або тимчасового зберігання конфіденційних даних застосовуйте USB-накопичувачі з вбудованим шифруванням, що забезпечить захист даних навіть при втраті пристрою.**
- **Перед завантаженням документів у хмарні сховища для зберігання зашифруйте їх, щоб забезпечити додатковий рівень захисту.**
- **Під час віддалених зустрічей обирайте платформи з підтримкою шифрування (наприклад, Zoom із налаштуваннями шифрування або Microsoft Teams) для захисту конфіденційності комунікацій.**

Безпечна передача інформації

- Не використовуйте публічний Wi-Fi (мережу без пароля), оскільки зловмисники також можуть отримати до неї доступ і перехопити інформацію.
- Застосовуйте захищені канали зв'язку (наприклад, VPN із шифруванням) для передачі конфіденційних даних.
- Підписуйте цифрові підписи та шифруйте файли перед відправкою, щоб ніхто, крім вас і отримувача, не зміг їх прочитати, отримувач був впевнений у відправнику.
- Не зберігайте конфіденційну інформацію в поштових скриньках або месенджерах.
- Перевіряйте адресу отримувача, щоб упевнитися, що дані надсилаються правильному адресату.
- Мінімізуйте час зберігання конфіденційної інформації в мережі Інтернет до мінімально необхідного періоду її використання.

Дякую за увагу!

Основні ідеї, які варто запам’ятати:

- Завжди обирайте безпечні засоби комунікації.
- Не довіряйте нікому й нічому автоматично.
- Використовуйте цифрові підписи та шифрування.
- Мінімізуйте зберігання конфіденційних даних в Інтернеті.
- Видаляйте завершене електронне листування.
- Регулярно оновлюйте програмне забезпечення.
- Створюйте резервні копії важливих даних.