

АТАКА НА ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

Перша частина. Електронний підпис слугує засобом ідентифікації особи в цифровому середовищі і забезпечує цілісність, автентичність та неможливість заперечення авторства документів. Існують три основні категорії електронних підписів [1].

Простий електронний підпис: базова форма, яка може бути представлена у вигляді зображення підпису. Має обмежену юридичну силу, здебільшого використовується для внутрішніх документів.

Удосконалений електронний підпис: використовує криптографію для забезпечення безпеки і автентичності. Має вищу юридичну силу порівняно з простим підписом і використовується для важливіших угод.

Кваліфікований електронний підпис: найбезпечніший варіант, створюється за допомогою сертифікованого електронного ключа, має таку ж юридичну силу, як власноручний підпис.

Основні характеристики ЕП:

- безпека: криптографічні методи забезпечують цілісність підписаних документів;
- автентифікація: дає змогу ідентифікувати підписанта;
- юридична сила: у багатьох країнах має рівнозначну силу з паперовим підписом, якщо відповідає стандартам.

Застосування ЕП:

- державні послуги: подача електронних заяв та отримання документів;
- бізнес: укладання контрактів і обробка фінансових документів;
- фінансовий сектор: електронні банківські операції та оформлення кредитів;
- право: реєстрація прав власності та подання судових документів.

Чому важливо захищати ЕП [2]:

- запобігання шахрайству: крадіжка або підробка підпису може призвести до виготовлення підроблених документів;
- цілісність даних: гарантує, що інформація не була змінена після підписання;
- юридична сила: підроблений підпис може призвести до юридичних спорів;
- конфіденційність: захист даних від несанкціонованого доступу;

- довіра до систем: надійний захист сприяє розвитку електронних документів і онлайн-сервісів;

Захист електронного підпису є критично важливим для запобігання фінансовим втратам і підтримання довіри до цифрових рішень.

Друга частина. Атаки на електронний підпис – основні види [3]:

- криптографічні атаки (аналіз алгоритмів підпису): невразливість алгоритмів підпису може бути скомпрометована шляхом криптоаналізу. Зловмисники можуть намагатися знайти слабкі місця в алгоритмах, таких як RSA, DSA або ECDSA, для відновлення приватного ключа або створення підроблених підписів;

- викрадення закритого ключа: закритий ключ є ключовим елементом генерації електронного підпису. Якщо зловмисник отримує доступ до закритого ключа (через витік даних, шкідливе програмне забезпечення або ненадійну безпеку), він може підписувати документи від імені власника.

- фішингові атаки та соціальна інженерія: зловмисники можуть використовувати фішингові атаки для викрадення облікових даних користувачів або ще більш критично – закритих ключів. Соціальна інженерія може включати маніпуляції з метою переконання жертви надати доступ до ключів чи паролів;

- атаки на алгоритми хешування: якщо хеш-функція, що використовується для створення електронного підпису, має вразливості, зловмисник може знайти колізії або відтворити підпис підробленого документа. Це може скомпрометувати цілісність підписаних даних.

Захист від атак на електронний підпис [4]:

- використання сильних криптографічних алгоритмів: вибирайте сучасні, перевірені алгоритми з достатньою довжиною ключа (наприклад, ECDSA з 256-бітним ключем), щоб зменшити ризик криптографічних атак;

- використання двофакторної аутентифікації (2FA): додайте додатковий рівень безпеки для доступу до рахунків і систем, які використовують електронні підписи, щоб ускладнити доступ для зловмисників;

- навчання користувачів: проводьте регулярні тренінги з безпеки, щоб навчити працівників розпізнавати фішингові атаки та інші форми соціальної інженерії, зокрема не натискати на підозрілі посилання.

Висновок. Електронний підпис є надзвичайно важливим компонентом сучасного цифрового середовища, що забезпечує ідентифікацію особи та цілісність документів. Однак із зростанням використання електронних підписів з'являються нові загрози, які можуть поставити під ризик їх безпеку. Основні категорії електронних підписів — простий, удосконалений і кваліфікований — надають різні рівні захисту та юридичної сили, що робить їх відповідними для різних видів угод та документів.

Атаки на електронні підписи, такі як криптографічні атаки, викрадення закритого ключа, фішингові атаки та атаки на алгоритми хешування, можуть призвести до серйозних наслідків, включаючи фінансові втрати і правові спори. Саме тому захист електронного підпису є критично важливим для підтримання довіри до цифрових рішень.

Для забезпечення їхньої безпеки необхідно впроваджувати сучасні криптографічні алгоритми, використовувати двофакторну аутентифікацію та проводити навчання користувачів, щоб знизити ризики, пов'язані з шахрайством і соціальною інженерією. Загалом, проактивний підхід до захисту електронних підписів допоможе запобігти їхньому зловживанню та як наслідок — зміцнити довіру до електронних послуг у суспільстві.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Види електронних підписів. URL: <https://instaco.com.ua/news/vidi-elektronnih-pidpisiv> (дата звернення: 18.04.2025).
2. Електронний підпис. URL: https://uk.wikipedia.org/wiki/Електронний_підпис (дата звернення: 18.04.2025).
3. Атаки на цифровий підпис. URL: https://stud.com.ua/170093/finansi/ataki_tsifroviy_pidpis (дата звернення: 18.04.2025).
4. Як захистити електронний підпис від шахраїв. URL: <https://litiko.com/uk/info-czentr-uk/statti/yak-zahystyty-elektronnyj-pidpys-vid-shahrayiv> (дата звернення: 18.04.2025).