Безпечне користування мережею Інтернет

План лекції

Вступ
1. Поняття, структура та класифікація комп'ютерних мереж
2. Інтернет-технології
3. Безпека браузерів
4. Електронний підпис

Висновки

Рекомендована література

Основна

1. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
2. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : BAITE, 2021. 106 с.
3. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : BAITE, 2021. 262 с.

Допоміжна

4. Про електронні комунікації: Закон України від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.
5. Про електронні документи та електронний документообіг: Закон України від 22.05.2003. Офіційний вісник України. 2003. № 25 (04.07.2003). ст. 1174.
6. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017. Офіційний вісник України. 2017. № 91 (21.11.2017). ст. 2764.
7. Інтернет-технології. URL: https://uk.wikipedia.org/wiki/Інтернет-технології.
8. Веб-сайт. URL: https://uk.wikipedia.org/wiki/Веб-сайт.
9. Електронна дошка оголошень. URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень.
10. Social bookmarking. URL: http://en.wikipedia.org/wiki/Social_bookmarking.
11. Skype. URL: https://uk.wikipedia.org/wiki/Skype.
12. Viber. URL: https://uk.wikipedia.org/wiki/Viber.

Інформаційні ресурси в Інтернеті

13. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

У своїй повсякденній діяльності користувачам нерідко доводиться мати справу з різними мережевими технологіями – як для здійснення специфічної службової діяльності, так і для комунікацій у цілому. В основному, середовищем, де це відбувається, є Інтернет.

1. Поняття, структура та класифікація комп'ютерних мереж

Для поняття «комп'ютерна мережа» більш загальним терміном є дефініція «електронна комунікаційна мережа», яка згідно зі ст. 2 Закону України від 16.12.2020 «Про електронні комунікації» є комплексом технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Як випливає із цього визначення, для організації роботи мережі потрібно використовувати певну сукупність апаратних та програмних засобів (кабелів, з'єднувачів, мережевих адаптерів, трансіверів, репітерів, концентраторів, комутаторів, маршрутизаторів, мостів, шлюзів тощо).

За територіальною ознакою комп'ютерні мережі поділяються на *локальні* (Local Area Networks – LAN), *міські* (Metropolitan Area Networks – MAN), *глобальні* (Wide Area Networks – WAN). Інколи в цій класифікації виділяють мережі *кампусні* (Campus Area Network – CAN) та *широкомасштабні* (Wide Area Network – WAN).

Одним з ключових елементів організації сучасних комп'ютерних мереж є відповідна система адресації. Найбільш поширеною подібною системою є адресація з використанням стеку протоколів TCP/IP.

У стеку TCP/IP використовуються три типи адрес:

- апаратні (найпоширенішими є MAC-адреси, проте можуть використовуватися адреси IPX і X.25);
- IP-адреси;
- доменні імена.

MAC-адреса, яка складається з 6 байт, призначається мережевим адаптерам і мережевим інтерфейсам. Вона функціонує у межах локальної мережі.

Уся множина комп'ютерів ідентифікується за допомогою IP-адрес, яка для IPv4 складається з 32 біт (4 октети по 8 біт, розділених крапками), а для IPv6 – зі 128 біт. IP-адреса призначається окремим інтерфейсам, тому якщо один комп'ютер (хост) містить кілька інтерфейсів, він може мати і кілька IP-адрес. IP-адреса складається з двох частин: старшої (ліворуч) – мережевої, яка визначає номер мережі, і молодшої (праворуч) – хостової, яка визначає номер хоста в цій мережі.

Для організації роботи з IP-адресами використовуються дві основних моделі: класова (для IPv4 – класи A, B, C, D і E) та безкласова. Для того, щоб відрізнити хостову та мережеву частину, в IP-адресі може використовуватися або маска мережі (стандарт IPv4), або префікс мережі (визначається слешем « / » в обох стандартах).

Для того, щоб спростити процес ідентифікації для людини, в мережі використовуються доменні імена. Інформацію про асоційовані з доменними іменами IP-адреси надають служби імен доменів (DNS). У мережі існує ієрархія доменів, так само як і ієрархія служб DNS.

2. Інтернет-технології

Інтернет-технології – це технології створення і підтримки різних інформаційних ресурсів у комп'ютерній мережі Інтернет. Найбільш поширеними *програмними технологіями,* які використовуються для вчинення протиправної діяльності у кіберсфері, є:

- спеціально створені веб-сайти;
- дошки оголошень (www.ss.ua, olx.ua, www.ria.com, www.sudver.com, inforico.ua, www.doshka.net, k4.at.ua, www.stop.kiev.ua, www.ukrboard.com.ua);
- комп'ютерні соціальні мережі (Facebook, Twitter, LinkedIn, Instagram, TikTok);
- електронна пошта (Evolution, KMail, Mozilla Thunderbird, Netscape Mail, Outlook Express, TheBat!);
- чати (http://www.e-chat.co/, http://tinychat.com/, http://www.ukranianwomendating.com/, http://www.wireclub.com/places/ukra);
- мультимедійні засоби спілкування (MSN, Google Talk, Pidgin, AIM, Trillian, Windows Live Messenger, Yahoo Messenger, Skype, Viber, WhatsApp);
- засоби забезпечення анонімності (Proxy servers (HTTP, SOCKS, CGI), Dark-net, Tor, 2IP);
- засоби шифрування (PGP, Red Phone, Truecrypt);
- засоби стеганографії;
- мережеві сховища (хмари, Peer-to-peer, FTP, відеохостинги);
- електронні гроші (PayPal, Bitcoin, Paxum);
- площадки, які можуть бути використані для легалізації коштів (WesternUnion, Forex);
- шкідливе програмне забезпечення.

Розглянемо докладніше окремі технології, які можуть бути використані для вчинення протиправних дій.

Веб-сайт – це сукупність веб-сторінок, доступних у мережі Інтернет, які об'єднані як за змістом, так і за навігацією.

Веб-сайти нерідко застосовуються зі злочинною метою. Це може бути купівля / продаж за їх допомогою викраденої інформації або заборонених

до використання предметів і речовин, поширення протиправного контенту, подання оголошень щодо вчинення певних дій протиправного характеру тощо.

Електронна дошка оголошень – це веб-сайт, цілком аналогічний звичайним побутовим дошкам оголошень або рекламним газетам. Її вміст – це набір оголошень комерційного та/або некомерційного характеру, які розміщуються як на оплатній, так і на безоплатній основі, залежно від конкретного сайту. Багато рекламних компаній, що мають паперові видання і працюють у сфері теле- і радіореклами, також створюють і підтримують власні електронні дошки оголошень.

Електронна дошка оголошень зазвичай поділена на кілька тематичних розділів – відповідно до змісту оголошень. Як правило, це – продаж/купівля товарів, надання послуг, пошук/пропонування роботи тощо.

Для розміщення свого оголошення користувачеві потрібно лише ввести в спеціальній формі його тему, своє ім'я/псевдонім або назву організації, а також координати: адресу електронної пошти, поштову адресу, телефон, свій сайт тощо (набір даних залежить від конкретного ресурсу).

Після публікації оголошення воно відображається у відповідному розділі, і разом з ним, як правило, відображаються ім'я автора, його тема та зміст, а також контактні дані.

Електронні дошки оголошень бувають двох видів: ті, що модеруються (ті, у яких є так званий модератор – людина, яка контролює роботу цієї дошки), і ті, що не модеруються, – вони працюють автоматично.

В умовах стрімкого розвитку високих інформаційних технологій дошки оголошень стали потужним інструментом інтернет-реклами. Все більше людей купують/продають товари та послуги через Інтернет, використовуючи для цього дошки оголошень. Український сегмент мережі Інтернет не є винятком і налічує сотні різних дошок оголошень, і ось найпопулярніші з них: www.ss.ua, olx.ua, www.ria.com, www.sudver.com, inforico.ua, www.doshka.net, k4.at.ua, www.stop.kiev.ua, www.ukrboard.com.ua тощо.

Для вчинення протиправних дій у кіберсфері нерідко застосовуються **комп'ютерні соціальні мережі.** Термін «соціальні мережі» – відносно нове явище інформаційних технологій, що має різні визначення. Технології соціальних мереж набувають різноманітних форм і, по суті, засновані на мережевих інтернет-технологіях, включаючи електронні журнали та інтернет-форуми, веб-журнали, соціальні блоґи, мікроблоґи, вікі, соціальні медіа, підкасти, фотографії або зображення, відео, рейтинги та соціальні закладки. Найбільш популярними соціальними мережами в Україні є Facebook, Twitter, LinkedIn, Instagram, TikTok, ClubHouse.

З точки зору криміналу, сайти соціальних мереж створюють надзвичайно зручну платформу для глобальних форумів, на яких правопорушники можуть провадити свою протиправну діяльність, майже не ризикуючи бути впійманими.

Соціальні медіа пропонують злочинцям елемент анонімності й прикриття, тому вони можуть спілкуватися на ранньому етапі своєї діяльності, майже не ризикуючи, що їх виявлять правоохоронні органи.

Електронна пошта (email, e-mail) – це метод обміну цифровими повідомленнями між одним автором та одним або більше отримувачем. Сьогодні системи електронної пошти спираються на модель проміжного накопичення і передачі, а сервери електронної пошти приймають, передають, доставляють і зберігають повідомлення. Ані користувачі, ані їх комп'ютери не повинні перебувати в онлайн-режимі одночасно – їм потрібно лише ненадовго з'єднатися з поштовим сервером на час, потрібний для відправлення або прийому повідомлень.

Користуватися послугами електронної пошти можна як через інтернет-браузер (Gmail, Yahoo, Hotmail, I.ua, Ukr.net), так і за допомогою спеціальних поштових клієнтів. Найпопулярнішими з них є: Mozilla Thunderbird, Outlook Express, TheBat!.

Повідомлення електронної пошти складається з двох частин:

1) *тіло повідомлення,* яке може містити текстову інформацію та інші дані, наприклад, графічні (фото/відео-, аудіо- (звукові) та бінарні (програми/додатки) файли. Також цілком можна включити гіперпосилання на інші джерела, такі як веб-сайти, групи новин та ftp-сайти;
2) *заголовок повідомлення,* який містить службову інформацію, у тому числі адресу електронної пошти відправника та одну або більше адрес одержувачів. Ці дані включають технічні деталі, наприклад те, хто надіслав повідомлення, за допомогою якої програми його було складено, а також через які поштові сервери пройшло повідомлення на шляху до одержувача.

Рівень сучасних технологій дозволяє швидко передавати значний обсяг медіа-контенту, тому серед правопорушників є досить популярними програмні **засоби медіа-спілкування.**

Одним із таких засобів є інтернет-пейджери (Instant Messengers) – це програми, які дозволяють обмінюватися текстовими повідомленнями між комп'ютерами у режимі реального часу.

Для спілкування також можуть використовуватись так звані «чати». Цей термін переважно застосовується для опису будь-якої форми синхронного конференц-зв'язку, а іноді – навіть асинхронного конференц-зв'язку. Отже,

цей термін може означати будь-яку технологію – від онлайн-чатів у реальному часі, онлайн-взаємодії з незнайомцями, обміну миттєвими повідомленнями та онлайн-форумів до повного занурення у графічне соціальне середовище. Основною метою чату є обмін текстовою інформацією з групою інших користувачів. Загалом здатність спілкуватися з багатьма людьми в рамках однієї бесіди відрізняє чати від програм обміну миттєвими повідомленнями, які переважно призначені для спілкування один-на-один. Користувачі певного чату зазвичай мають спільний інтерес або інший аналогічний зв'язок, а існуючі чати охоплюють широку низку тем. Нова технологія дозволяє передбачати в деяких програмах можливість обміну файлами та використання веб-камер.

Слід зазначити, що останнім часом правопорушники почали користуватися складнішими засобами спілкування, зокрема створеними на базі поширеного протоколу передачі даних VoIP. VoIP-протокол (протокол передачі голосу Інтернетом) та відеотелефонія є наступним кроком розвитку інтернет-технологій, а тому за своєю суттю переважно використовуються молоддю, особливо якщо цю технологію вбудовано у певні соціальні медіа, і вони присутні на планшетах чи смартфонах.

Найпопулярнішими застосунками такого штибу є Skype, Telegram, WhatsApp, Viber.

3. Безпека браузерів

Що таке інтернет-браузер? Це – програмне забезпечення, яке дозволяє користувачам отримувати інформацію з сайтів мережі Інтернет. Браузери транслюють код інтернет-сторінок у зрозумілий для людини вигляд. Для передачі використовується протокол HTTP або його безпечніша версія HTTPS. Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо) через мережу Інтернет. Приклади браузерів: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari.

Але браузери наразі не тільки надають доступ до сторінок, а і слугують платформою для додаткових програм, що полегшують користування мережею Інтернет. Ці програми називаються плагінами. Плагіни розширюють функціональність браузера, додаючи додаткових функцій. Більшість плагінів можуть встановлювати додаткові панелі інструментів, маркетинг і помічників пошуку. Крім того, ви може помітити нові кнопки, посилання або функції, такі як блокування спливаючих вікон, доданих у браузер. Деякі плагіни невидимі для користувача, оскільки вони працюють у фоновому режимі й не мають графічного інтерфейсу. Деякі з плагінів можуть бути шкідливими. Щоб пам'ятати вас, браузери використовують таку річ, як cookies.

Cookies – це невеликі текстові файли у нас на комп'ютерах, у яких зберігається інформація про ваші попередні дії на сайтах. Крім входів до акаунтів, вони вміють запам'ятовувати:

- налаштування користувачів: наприклад, мова, валюта або розмір шрифту;
- товари, які ви переглядали або додали до кошика;
- текст, який ви вводили на сайті раніше;
- IP-адресу і місце розташування користувача;
- дату і час відвідування сайту;
- версію ОС і браузера;
- кліки та переходи.

Коли ми робимо на сайті якісь дії, наприклад, додаємо товар до кошика або вводимо дані входу до акаунту, сервер записує цю інформацію в cookies і відправляє браузеру разом зі сторінкою. Коли ми переходимо на іншу сторінку сайту або заходимо на нього через деякий час, браузер відправляє cookies назад.

Cookies бувають тимчасовими і постійними. Постійні cookies залишаються на комп'ютері, коли ми закриваємо вкладку з сайтом, а тимчасові – видаляються. Які саме cookies використовувати на конкретному сайті – тимчасові або постійні – вирішує його розробник. Саме тому на одних сайтах ми не виходимо з акаунтів, навіть коли заходимо на них раз через кілька днів, а на інших вводимо пароль заново, хоча відійшли від комп'ютера на п'ять хвилин. Самі по собі cookies не є небезпечними – це звичайні текстові файли. Вони не можуть запускати процеси на комп'ютері та взагалі взаємодіяти з операційною системою. Але їх можуть спробувати перехопити або вкрасти, щоб відстежувати ваші попередні дії в мережі або входити до ваших акаунтів без авторизації.

Зазвичай інформацію, яку записують у cookies, зашифровують перед відправкою, а власне cookies передають за HTTPS-протоколом. Це допомагає захистити призначені для користувача дані, але за впровадження шифрування і безпечну відправку відповідає розробник сайту. Відвідувачам залишається тільки сподіватися, що все налаштували грамотно. Зі свого боку, користувач може тільки заборонити браузеру використовувати cookies або час від часу чистити їх самостійно.

Зовсім відключати cookies – не завжди хороша ідея. Наприклад, усі інтернет-магазини працюють за допомогою cookies. Якщо заборонити браузеру їх використовувати, сервер не зможе запам'ятати, що саме ви додали до кошика. Чистити cookies вручну практичніше, але доведеться щоразу заново налаштовувати зовнішній вигляд сайту і входити до акаунтів.

Чому через браузер можуть реалізовуватись загрози?
Браузери застарівають та з'являються вразливості, які експлуатуються хакерами віддалено.

Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, а ви можете навіть не знати про те, що стали жертвою.

Зловмисники зламують публічні точки доступу до мережі Інтернет і намагаються перехопити інформацію користувачів.

Якщо ви звернете увагу на новини зі світу кібербезпеки, то побачите, що браузери майже щомісяця публікують оновлення та звітують про винайдені та закриті вразливості. Чому? Тому що дуже велика кількість вразливостей виявляється ледь не щоденно. І хакери одразу починають їх використовувати у своїх атаках.

Треба зрозуміти, що не існує абсолютно безпечного браузера. Іноді виникає ситуація, коли вразливості можуть залишатися незакритими протягом десятиліть. Тобто ви, щоб не стати жертвою, маєте ретельно піклуватись про безпеку вашого браузера. Але треба пам'ятати, що ваша необачність може нести ризики не тільки вам особисто, а й усій вашій установі.

З метою убезпечення браузера необхідно постійно його оновлювати, щоб не допустити появи відомих вразливостей у ньому. Також необхідно коректно налаштувати вимоги до приватності даних у браузері. Встановити додаткові плагіни безпеки, наприклад, HTTPS Everywhere (буде попереджати, якщо сайт не захищено HTTPS і є ризик перехоплення даних – логінів, паролів тощо) або AdBlock (блокувальник реклами).

4. Електронний підпис

Одним із сучасних інструментів убезпечення в мережі Інтернет є електронний підпис. Згідно зі ст. 5 Закону України «Про електронні документи та електронний документообіг» ***електронний документ*** – це документ, інформація в якому зафіксована у вигляді електронних даних, враховуючи **обов'язкові реквізити документа.**

Реквізитом електронного документа є ***електронний підпис*** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис.

Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа.*

При цьому ***особистий ключ*** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Згідно зі ст. 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» залежно від ступеня довіри до засобів електронної ідентифікації вводяться три рівні електронного підпису:

- простий електронний підпис та печатка – низький рівень довіри;
- удосконалений електронний підпис та печатка – середній рівень довіри;
- кваліфікований електронний підпис та печатка – високий рівень довіри.

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, а також презумпцію його відповідності власноручному підпису. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

Перехід до використання на практиці електронного підпису є черговим важливим кроком на шляху втілення електронного урядування, адже електронний підпис є важливим компонентом електронного документообігу.

Упровадження електронного підпису, зокрема, робить можливим:

- подання різноманітної бухгалтерської, податкової, статистичної та іншої звітності до державних органів в електронному вигляді телекомунікаційними каналами, зокрема через Інтернет;
- організацію онлайн-закупівель державних суб'єктів господарювання через систему електронних торгів, що сприяє забезпеченню прозорості їх діяльності та зменшенню кількості випадків зловживань;
- юридично значущий електронний документообіг між органами державної влади, підприємствами й організаціями;
- отримання громадянами різноманітних офіційно засвідчених документів та участь у виборах через мережу Інтернет.

Загальна схема накладання електронного підпису наведена на рис. 1, а його перевірки – на рис. 2.

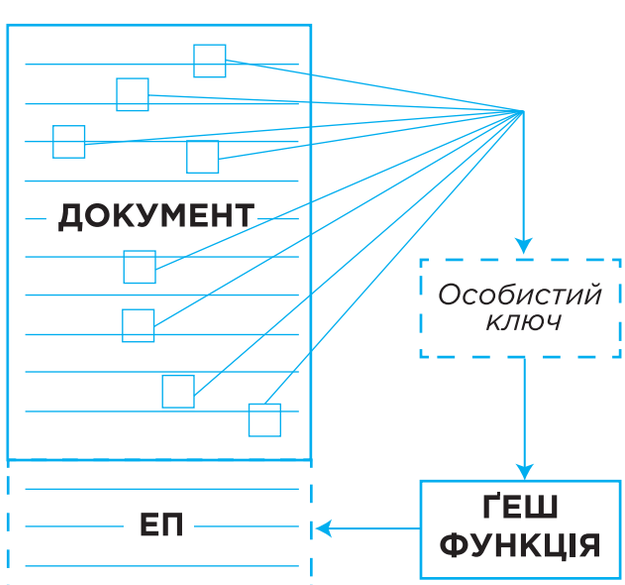
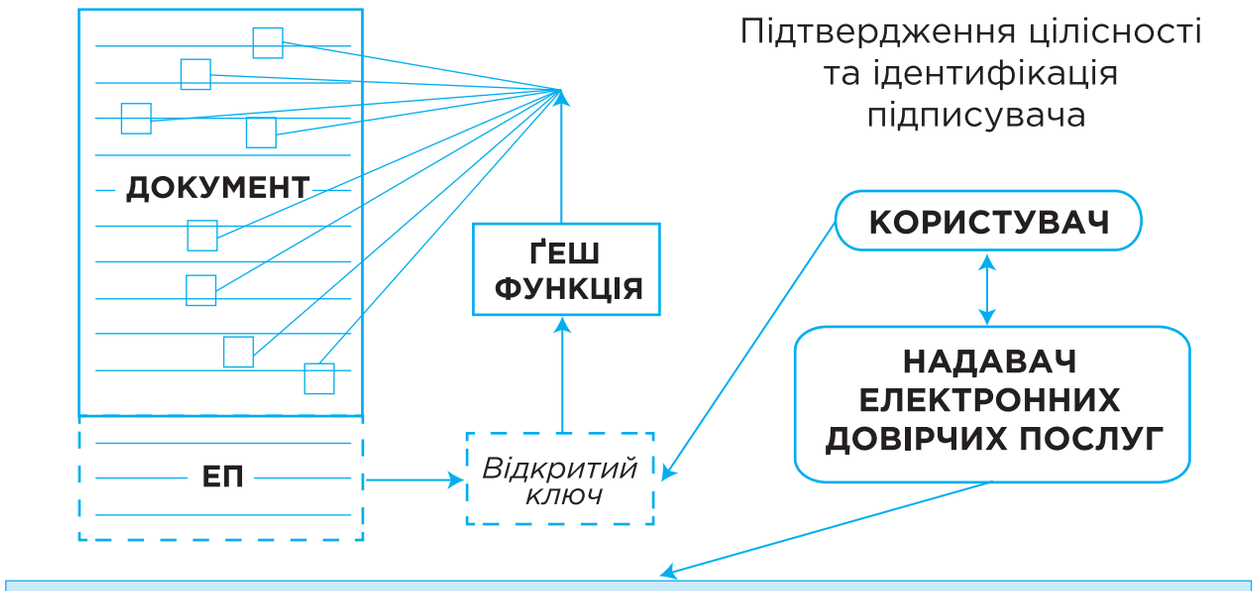


Рис. 1. Приблизна модель накладання електронного підпису



КВАЛІФІКОВАНИЙ СЕРТИФІКАТ КЛЮЧА

- позначка, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;
- позначка, що сертифікат відкритого ключа виданий в Україні;
- ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа;
- ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг;
- місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;
- значення відкритого ключа, який відповідає особистому ключу;
- відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;
- серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;
- кваліфікований електронний підпис або кваліфікована електронна печатка, створені суб'єктом, який видав сертифікат;
- відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;
- відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;
- відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації веб-сайту).

Рис. 2. Приблизна модель перевірки електронного підпису

Підсумовуючи викладене, необхідно зазначити, що накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується,** але при цьому можна впевнитись у *цілісності* документа й *ідентифікувати його підписувача.*

Висновки

Як головні правила убезпечення в мережі Інтернет можна запропонувати такі:

1. Налаштуйте браузер на безпечний перегляд сторінок.
2. Не завантажуйте підозрілі файли.
3. Використовуйте антивірус та фаєрвол.
4. Шифруйте повідомлення.
5. Використовуйте захищені з'єднання.
6. Встановлюйте оновлення.