ТЕМА Ідентифікація і автентифікація користувачів.

І. Поняття про ідентифікацію користувача та її особливості

Ідентифікація – привласнення суб'єктам або об'єктам доступу ідентифікатора або порівняння пред'явленого ідентифікатора з переліком привласнених ідентифікаторів.

Ідентифікація об'єкта - це його впізнання, ототожнення із чим-небудь. Якщо ж говорити про області інформаційних технологій, то даний термін звичайно означає встановлення особистості користувача. Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу до закритої інформації тощо. Таким чином, ідентифікація є одним з основних понять в інформаційній безпеці.

Сьогодні існує декілька способів ідентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші - в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно думати, який спосіб ідентифікації реалізовувати в продуктах.

Існує три найпоширеніших види ідентифікації:

1. Парольна ідентифікація

Ще не дуже давно парольна ідентифікація була чи ледве не єдиним способом визначення особистості користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного. Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використовуються пари: логін-пароль). Далі при кожній спробі входу людина повинна вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує.

Недоліком парольної ідентифікації є значна залежність надійності ідентифікації від користувачів, точніше від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Фахівці в

області інформаційної безпеки радять використовувати довгі паролі, що складаються з безладного сполучення букв, цифр і різних символів.

2. Апаратна ідентифікація

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі. На даний момент найбільше поширення одержали два типи пристроїв. До першого ставляться всілякі карти. Їх досить багато, і працюють вони за різними принципами. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксі іті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти - аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д

Іншим типом ключів, які можуть використатися для апаратної ідентифікації, є так звані токени . Ці пристрої мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT).

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте для введення в експлуатацію системи майнової ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися або можуть бути загублені користувачами.

3. Біометрична ідентифікація

Біометрія - це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних

біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості виверти. Так що зловмисникам доводиться видумувати все нові й нові способи обману біометричних сканерів.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Варто також відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві доводиться вибирати, який пристрій придбати - дорожчий й кращий або дешевший й гірший.

Багатофакторна ідентифікація. Поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів.

Причому комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використається тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбору його пароля зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

II. Основні принципи та методи автентифікації

Автентифікацією – називається процедура верифікації належності ідентифікатора суб'єкту.

Автентифікація здійснюється на основі того чи іншого секретного елемента (автентифікатора), який є у розпорядженні як суб'єкта, так і інформаційної системи. Звичайно, інформаційна система має в розпорядженні не сам секретний елемент, а деяку інформацію про нього, на основі якої приймається рішення про адекватність суб'єкта ідентифікатору. Наприклад, перед початком інтерактивного сеансу роботи більшість операційних систем запитують у користувача його ім'я та пароль. Введене ім'я є ідентифікатором користувача, а його пароль - автентифікатором. Операційна система зазвичай зберігає не сам пароль, а його хеш-суму, що забезпечує складність відновлення пароля.

В інформаційних технологіях використовуються такі методи автентифікації:

- однобічна автентифікація, коли клієнт системи для доступу до інформації доводить свою автентичність;

- двобічна автентифікація, коли, крім клієнта, свою аутентичність повинна підтверджувати і система (наприклад, банк);

- трибічна автентифікація, коли використовується так звана нотаріальна служба аутентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Методи аутентифікації також умовно можна поділити на дно факторні та двох факторні.

дно факторні методи діляться на:

- *логічні* (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);

- *ідентифікаційні* (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, тарт-карта, штрих-кодова карта тощо. Недоліки: для зчитування інформації з фізичного об'єкта (носія) необхідний спеціальний рідер; носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію).

- *біометричні* (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліки: біометричні методи дорогі і складні в обслуговуванні; чутливі до зміни параметрів носія інформації; володіють низькою достовірністю; призначені тільки для автентифікації людей, а не програм або інших ресурсів).

Автентифікація за відбитками пальців. Ця біометрична технологія, цілком імовірно, в майбутньому використовуватиметься найширше. Переваги засобів доступу по відбитку пальця - простота використання, зручність і надійність. Весь процес ідентифікації здійснюється досить швидко і не вимагає особливих зусиль від користувачів. Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами.

Використання геометрії руки. Цей метод сьогодні застосовується в більш ніж 8000 організацій, включаючи Колумбійський законодавчий орган, Міжнародний Аеропорт Сан-Франциско, лікарні і імміграційні служби. Переваги ідентифікації по геометрії долоні порівнянні з автентифікацією по відбитку пальця в питаннях надійності, хоча пристрій для зчитування відбитків долонь займає більше місця. Найбільш досконалий пристрій, Handkey, сканує як внутрішню, так і бічну сторону руки.

Автентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що зразок плям на оболонці знаходиться на поверхні ока, і від користувача не вимагається спеціальних зусиль. Фактично відео зображення ока може бути від скановане на відстані метра, що робить можливим використання таких сканерів в банкоматах. Ідентифікуючі параметри можуть скануватися і кодуватися, зокрема, і у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Автентифікація за сітківкою ока. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули великого поширення в надсекретних системах контролю доступу, оскільки ці засоби атентифікації характеризуються одним з найнижчих відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу.

Автентифікація за рисами особи (за геометрією особи) - один з напрямів, що швидко розвиваються, в біометричній індустрії. Розвиток цього напряму пов’язаний з швидким зростанням мультимедійних відео-технологій. Проте більшість розробників поки зазнають труднощі в досягненні високого рівня виконання таких пристроїв. Проте можна чекати появу в найближчому майбутньому спеціальних

пристроїв ідентифікації особи за рисами обличчя в залах аеропортів для захисту від терористів і т. ін.

Двох факторні методи автентифікації отримують в результаті комбінації двох різних одно факторних методів, частіше всього ідентифікаційного та логічного. Наприклад: «пароль + дискета», «магнітна карта + PIN».

Кожен клас методів має свої переваги і недоліки. Майже всі методи аутентифікації страждають на один недолік - вони, насправді, автентифікують не конкретного суб'єкта, а лише фіксують той факт, що автентифікатор суб'єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації автентифікатора.

Тема Електронний цифровий підпис.

Поняття та визначення електронного цифрового підпису

Статтею 1 Закону України "Про електронний цифровий підпис" визначено такі терміни:

електронний підпис -дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

електронний цифровий підпис -вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача . Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

сертифікат відкритого ключа (далі - сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

акредитація – процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов’язану з обслуговуванням посилених сертифікатів ключів;

компрометація особистого ключа - будь-яка подія та/дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється в порядку, визначеному законодавством.

Власноручний підпис та електронний цифровий підпис

Документ у традиційному розумінні цього поняття передбачає наявність носія інформації, за допомогою якого забезпечується сприймання інформації тільки органами чуттів людини (зір, слух тощо).

Підпис, який проставляється автором документа на папері (власноручний підпис), – це рукописне, та іноді графічно стилізоване ім'я або інший графічний знак, що ідентифікує автора (підписувача), і означає його згоду зі змістом документа. Перевірка справжності власноручного підпису здійснюється шляхом його візуального звірення з оригіналом, який зафіксований у встановленому порядку. За необхідності для офіційної перевірки підпису може бути здійснена відповідна експертиза.

На відміну від документа на папері, електронний документ (ЕД) дуже легко може бути підданий різним змінам. Тому, для гарантії забезпечення можливості здійснення контролю справжності підпису, накладеного на ЕД, необхідно застосовувати відповідний механізм, який дає змогу однозначно визначити, чи вносилися будь-які несанкціоновані автором зміни до вмісту ЕД після його підписання.

Накладання підпису на ЕД шляхом графічного відтворення власноручного підпису не може слугувати підтвердженням того, що документ санкціонований підписувачем, оскільки графічний образ може бути скопійований і проставлений під будь-яким текстом або іншим елементом ЕД, і тим самим підписувачу буде приписане незаконне авторство документа.

Для ЕД повним аналогом власноручного підпису під документом на папері на сьогодні є електронний цифровий підпис (ЕЦП), Застосування якого реалізується за допомогою інформаційних технологій і здійснюється шляхом певних криптографічних перетворень над ЕД (набором електронних даних), на основі яких

відтворюється вміст цього ЕД. За визначених законодавством умов ЕЦП прирівнюється до власноручного підпису і має однакову з ним юридичну силу.

Ключі електронного цифрового підпису

Технологія застосування ЕЦП базується на методах криптографії. З цієї сфери було присвоєно термін "ключ", тобто набір двійкових даних фіксованої довжини. У практичній криптографії використовується пара пов'язаних між собою ключів – ключ для шифрування і, відповідно, для дешифрування. Зазначені дані слугують параметрами для відповідних алгоритмів криптографічних перетворень. У сфері застосування ЕЦП використовується аналогічна пара – особистий ключ (ОК) і відкритий ключ (ВК), перший з якої застосовується для накладання підпису, а другий – для його перевірки. Ця пара ключів створюється шляхом їх генерації за допомогою засобів ЕЦП на основі алгоритмів отримання випадкових чисел великої розрядності. При цьому до надійного засобу ЕЦП висувається, зокрема, вимога, з якою за його допомогою пара ключів може бути практично з генерована лише один раз, а їх захищеність має бути достатньо гарантованою – зокрема після перенесення ключів, з генерованих за допомогою цього засобу, на зовнішній носій інформації. Ці дані в такому засобі (наприклад персональний комп'ютер) будуть знищені, тобто стануть у подальшому недоступними. Крім того, технології використання надійного засобу ЕЦП повинні забезпечувати з достатньою гарантованістю, що ключі не можуть бути отримані похідними способами, а сам підпис є захищеним від підробки шляхом використання наявних інформаційних технологій.

Слід зазначити, що терміну "***особистий ключ***", тобто ключ, який повинен використовуватися особисто, із закриттям доступу до нього інших осіб, в англійській мові відповідає термін – "***private key".***

Важливість значення ОК у застосуванні ЕЦП підкреслюється у відповідних положеннях законодавства. Зокрема, відповідно до статті 7 Закону України "Про електронний цифровий підпис", підписувач (власник ОК) зобов'язаний зберігати ключ у таємниці, а відповідно до статті 8 – зберігання ОК підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

У законодавстві немає вимоги до форми зберігання ВК, за допомогою якого перевіряється ЕЦП. Він може зберігатися, зокрема, на папері – у вигляді запису

відповідного коду, а також на традиційних електронних носіях інформації – дисках, флешок, апаратних носіях тощо. На сьогодні на ринку присутні, апаратні носії ключової інформації, які призначені, зокрема, для збереження і використання ВК та апаратної реалізації криптографічних перетворень, і які виготовляються у формі, що зовні виглядає як флешка з USB - інтерфейсом. Апаратні носії ключової інформації забезпечують захищеність процесу виконання криптографічних перетворень, які здійснюються з використанням ОК, та унеможливлюють доступ до нього з боку апаратно-програмного середовища комп'ютера. За допомогою апаратного носія можуть генеруватися та зберігатися в ньому ОК та ВК підписувача. При цьому ОК підписувача зберігаються у внутрішній пам'яті апаратного носія, де забезпечується їх захист від несанкціонованого доступу.

Національний банк України своїм листом рекомендував банкам України розглянути питання щодо зменшення ризиків під час використання інформаційних технологій та програмно-технічних комплексів банків, зокрема, шляхом використання ряду апаратних носіїв ключової інформації систем криптографічного захисту інформації і погодив використання цих апаратних носіїв у системі криптографічного захисту інформації Національного банку.

Захищеність електронного цифрового підпису

Захищеність ЕЦП від відтворення чи підробки базується на застосуванні у відповідних технологіях методів криптографії. Так, у разі застосування алгоритму, визначеного ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння ", для формування та перевіряння електронного цифрового підпису з довжиною ключа у 264 біти тривалість часу, необхідного для його можливого "зламування" шляхом застосування найсучасніших методів крипто аналізу з допомогою комп'ютера із частотою процесора у 3 ГГЦ, експерти оцінюють величиною майже 1 тис. років. Тобто такий тривалий час і лежить в основі гарантії стійкості ЕЦП. Крім того, додатковою перешкодою для зловмисників, які можуть здійснити спробу "зламування" ОК, є те, що термін його використання обмежується (як правило, не більше року) і підписувач періодично замінює ОК (одночасно з ним і ВК). Підписувач також може замінювати ОК і достроково – за наявності підозри про

його компрометацію, тобто виникнення ситуації, коли існує ймовірність того, що він став доступним іншій особі (особам).

Правовий статус електронного цифрового підпису

Відповідно до статті 1 Закону України "Про електронний цифровий підпис" ЕЦП накладається на набір електронних даних, який додається до цього набору або логічно з ним поєднується. Відповідно до статті 6 Закону України "Про електронні документи та електронний документообіг" електронний підпис є обов'язковим реквізитом ЕД, який використовується для ідентифікації автора та/ підписувача ЕД іншими суб'єктами електронного документообігу. Слід зазначити, що використання ЕЦП дає змогу також підтвердити цілісність ЕД. При цьому необхідно підкреслити, що лише ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки), а інші види електронного підпису не мають такого статусу.

Відповідно до статті 5 Закону України "Про електронний цифровий підпис" органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності повинні застосовувати лише ЕЦП, а для засвідчення чинності ВК використовують лише ***посилений сертифікат відкритого ключа*** (ПСВК). При цьому слід зазначити, що відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" зазначені у ній установи ЕЦП не застосовують:

– для складання ЕД, які не можуть бути оригіналами у випадках, передбачених законодавством;

– для здійснення правочинів на суму, що перевищує1 млн. грн.

Електронна печатка

У разі, коли згідно із законодавством необхідне засвідчення справжності підпису печаткою на документах та відповідності копій документів оригіналам, застосовується спеціально призначений для таких цілей ЕЦП, який називається ***електронною печаткою*** (ЕП). Хоча із суто технологічного погляду ЕЦП і ЕП цілком аналогічні, одночасна наявність цих об'єктів у законодавстві про ЕД зумовлена різними функціями, які повинні забезпечуватися за їх допомогою, і викликано,

зокрема, існуванням двох різних типів суб'єктів, яких умовно можна назвати "директор" і "секретар". Представники першого типу суб'єктів підписують документ, а представники другого – скріплюють підпис печаткою.

Відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" зазначені у її назві установи застосовують ЕП лише за наявності у них відповідної печатки, що використовується для документів на папері. При цьому у ПСВК, що використовується установою для ЕП, додатково зазначається спеціальне призначення ЕЦП та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці (так звана "мокра" печатка). Право проставляння ЕП на ЕД надається лише тому працівнику установи, який проставляє відповідну "мокру" печатку на документах на папері.

Цілком очевидно, що за відсутності у законодавстві поряд з положеннями про ЕЦП також положень і про ЕП, говорити про повноцінне використання ЕД нарівні з документами на папері неможливо.

Застосування ЕЦП й ЕП зокрема дасть змогу використовувати ЕД під час проведення виборів різних рівнів. При цьому стане можливим більш оперативне отримання Центральною виборчою комісією протоколів виборчих комісій в електронній формі, які міститимуть поряд з ЕЦП також й ЕП. Такі протоколи за своїм юридичним статусом матимуть рівну силу з документами на папері, на які проставлені власноручні підписи, скріплені "мокрою" печаткою.

Використання електронного цифрового підпису

Згідно із законодавством ЕЦП накладається на ЕД, а більш загально – на набір електронних даних і додається до цього набору або логічно з ним поєднується. Таким набором може бути файл, який являє собою вміст ЕД, сформованого, наприклад за допомогою текстового процесора Microsoft Word чи редактора електронних таблиць Microsoft Excel, текстовий, графічний, аудіо - або відео файл тощо.

Слід зазначити, що особистий ключ (ОК), відкритий ключ (ВК) й електронний цифровий підпис (електронна печатка) аналогічно з ЕД, як правило, формуються,

подаються і зберігаються в інформаційній системі і на персональному комп'ютері в електронному вигляді як файли з двійковими даними.

Накладання ЕЦП (ЕП) на ЕД (набір електронних даних) здійснюється за допомогою ОК, який слугує параметром для криптографічного перетворення цих даних. Початковим етапом цього криптографічного перетворення даних, або гешування (рос. – *хеширование*, англ. – *hashing*), яке називають також геш-функцією (функцією згортки), є отримання геш-значення (геш-коду) ЕД. Іноді геш-код називають ще дайджестом ("відбитком") повідомлення (англ. – *message digest*). При цьому геш-код має фіксовану довжину, є унікальним і однозначно представляє ЕД (набір електронних даних), які підписуються. Після цього за допомогою ОК підписувача, який також є кодом фіксованої довжини, здійснюється шифрування геш-коду ЕД і в результаті цього формується код фіксованої довжини, який, власне, і являє собою ЕЦП, накладений на ЕД. Цілком зрозуміло, що не існує оберненого до гешування перетворення, за допомогою якого з геш-коду ЕД (набору електронних даних) можна відтворити сам ЕД (рис. 1).

Рис. 1. ***Схема формування електронного цифрового підпису***

З урахуванням того, що ЕЦП являє собою код, тобто набір електронних даних у двійковій формі, "прочитати" безпосередньо з нього дані про особу підписувача неможливо. Для цього існує і використовується механізм, в основу якого покладено **сертифікат відкритого ключа (СВК),** що формується для кожного конкретного ВК одним з суб'єктів інфраструктури відкритого ключа (ІВК) – центром сертифікації

ключів (ЦСК)/акредитованим центром сертифікації ключів (АЦСК), або засвідчувальним центром.

Слід відзначити, що власноручні підписи, проставлені підписувачем на два різних документи на папері, однакові між собою. Хоча, строго кажучи, точного графічного спів падіння вони не мають, але за необхідності графологічна експертиза може підтвердити, що вони проставлені однією й тією ж особою. Це, на перший погляд, може сприйматися як певний парадокс, але на відміну від ситуації з власноручним підписом, два ЕЦП, накладені підписувачем на два різних ЕД (із застосуванням одного й того ж ОК), відрізняються один від одного. Тобто два відповідних набори електронних даних (коди), отримані при цьому, є різними. Якщо ж припустити, що один і той же код виступатиме ЕЦП для різних ЕД, то, враховуючи, що такий "підпис" може бути вільно скопійований, точніше – отриманий інший його примірник, стане можливим і його подальше тиражування для будь-якої кількісті інших "документів" без участі автора. Таким чином, авторові можна буде нав'язати ЕД, з яким він не згоден, але при цьому буде зобов'язаний нести за нього відповідальність. Це означатиме, що за такої ситуації застосування ЕДО з використанням ЕЦП втратить будь-який сенс.

Технології використання надійного засобу ЕЦП повинні забезпечувати з достатньою гарантованістю, що ОК підписувача не може бути відтворений з ЕД (набору електронних даних), його геш-коду та ЕЦП, накладеного на цей ЕД, або з сукупності таких наборів даних (для різних документів). Як уже зазначалося, тривалість часу, необхідного для реалізації можливості відтворення ОК шляхом застосування найсучасніших методів крипто аналізу з допомогою сучасного комп'ютера оцінюється фахівцями величиною, близькою до 1000 років.

Перевірка справжності ЕЦП (ЕП), накладеного на ЕД (електронний набір даних), здійснюється за допомогою ВК.

Першим кроком цієї процедури є дешифрування коду ЕЦП за допомогою коду ВК, в результаті чого отримується первісний геш-код ЕД, тобто той геш-код, який був обчислений під час накладання ЕЦП на ЕД. Потім обчислюється геш-код ЕД, що перевіряється зараз, оскільки невідомо, чи збігається цей ЕД за вмістом із тим, ЕД, який підписувався.

Рис. 2. ***Схема перевірки справжності електронного цифрового підпису***

Після цього порівнюються ці два геш-коди і за позитивними результатами порівняння робиться висновок про справжність ЕЦП і цілісність ЕД (набору електронних даних), тобто про те, що після накладання ЕЦП на ЕД до нього не вносилося жодних змін.

Перевірка справжності ЕП, проставленої на ЕД, здійснюється за такою самою процедурою, що й перевірка ЕЦП (рис. 2).

Слід зазначити, що зміни, внесені до ЕД, точніше до відповідного набору електронних даних, можуть бути, зокрема, наслідком:

– умисної модифікації або знищення даних, здійснених певною особою;

– впливу шкідливої комп'ютерної програми, тобто ураження комп'ютерним вірусом;

– збою, тобто виходу зі штатного й переходу в позаштатний режим роботи інформаційної системи в цілому, або окремого комп'ютера, чи їх "зависання";

– дії технічних завад на електричні сигнали, за допомогою яких через телекомунікаційні канали передавалися ці дані.

Відповідно до статті 1 Закону України "Про електронний цифровий підпис" ЕЦП дає змогу перевірити цілісність електронних даних, на які він накладений, та

ідентифікувати особу підписувача. Оскільки ЕЦП являє собою код, то для отримання даних про особу підписувача використовується механізм сертифікату відкритого ключа (СВК). При цьому СВК (ПСВК) являє собою документ, виданий ЦСК (АЦСК, засвідчу вальним центром). Відповідно до статті 1 зазначеного Закону цей документ засвідчує чинність і належність ВК підписувачу. При цьому СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. Склад СВК визначено у статті 6 цього Закону. Він містить, зокрема, основні дані (реквізити) підписувача – власника ОК, а також ВК, який є парним до цього ОК, що означає, що ці ключі були з генеровані разом.

Якщо після перевірки справжності ЕЦП, накладеного на ЕД, за допомогою ВК, який міститься у СВК, буде отриманий позитивний результат, то дані про підписувача у СВК якраз й ідентифікують цю особу. Таким чином і співставляється, власне, код (ЕЦП) з особою підписувача. При цьому, хоча два коди (ЕЦП), накладені за допомогою одного й того ж ОК підписувача на два різних ЕД, будуть різними, перевірка їх справжності здійснюється за допомогою одного й того ж ВК. За позитивного результату перевірки буде ідентифікована одна й та ж особа – підписувач, дані про якого зазначені в СВК. Слід зазначити, що відповідно до статті 5 Закону України “Про електронний цифровий підпис” органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності ВК використовують лише ПСВК, які видаються АЦСК.

Відповідно до постанови Кабінету Міністрів України “Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності” справжність ЕЦП, накладеного на ЕД або інші електронні дані, та цілісність цього документа (електронних даних) перевіряється з дотриманням таких вимог:

– ЕЦП повинен бути підтверджений з використанням ПСВК за допомогою надійних засобів ЕЦП;

– під час перевірки повинен використовуватися ПСВК, чинний на момент накладення ЕЦП;

– ОК підписувача повинен відповідати ВК, зазначеному у ПСВК;

– на час перевірки повинен бути чинним ПСВК, сформований АЦСК та/ ПСВК відповідного засвідчувального центру.

Відмінності накладання електронного підпису на електронний документ від підписання документа на папері

Відповідно до статті 6 Закону України “Про електронні документи та електронний документообіг” накладанням електронного підпису завершується створення ЕД. Це означає, зокрема, що на цей момент в ЕД повинні бути присутніми усі необхідні елементи, включаючи його номер і дату підписання. На цю обставину слід звернути увагу під час впровадження і використання ЕД і ЕДО із застосуванням ЕЦП. Практика традиційного документообігу свідчить, що дата і номер зазвичай вносяться до документа на папері вже після його підписання. Внесення дати і номера до ЕД, на який вже накладено ЕЦП, порушить цілісність цього ЕД (набору даних) і при перевірці справжності ЕЦП буде отриманий негативний результат.

Позначка часу

Постановою Кабінету Міністрів України “Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу” визначено умови та вимоги до процедури засвідчення і створені правові засади для надання ЦСК відповідних послуг ЕЦП (точніше – послуг у сфері використання ЕЦП). У цьому Порядку визначено такі терміни:

послуга фіксування часу – процедура засвідчення наявності ЕД (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу;

позначка часу – сукупність електронних даних, створена за допомогою технічних засобів та засвідчена ЕЦП центру сертифікації ключів, яка підтверджує наявність ЕД (електронних даних) на певний момент часу.

Затвердженням зазначеного Порядку врегульовано функціонування ЦСК – довірених суб’єктів в ІВК, які повинні цілодобово надавати послуги зі створення позначок часу і мати при цьому точне й надійне джерело часу. У процесі фіксування

часу позначка часу (англ. – *Time Stamping*) додається або логічно поєднується з електронними даними таким чином, щоб була виключена можливість вносити до них зміни, а також зберігати позначки часу після надання послуги фіксування часу. Наявність позначки часу дає змогу перевірити достовірність часу наявності ЕД (електронних даних). При цьому можна використовувати СВК, який на момент перевірки ЕЦП, накладеного на ЕД, вже анульований або відкликаний. В іншому випадку, актуальність підписаного ЕД обмежена терміном дії СВК.

Спільним наказом Держкомінформнауки та Держспецзв'язку затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису (протокол фіксування часу)". Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмно-технічних комплексів АЦСК. Правильність реалізації протоколу та наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

Технічні специфікації визначають процедуру формування позначки часу, зокрема дії, які при цьому виконують користувач та ЦСК.

Згідно з процедурою, користувач попередньо обчислює геш-код (геш-значення) ЕД (електронного набору даних). Слід зазначити, що обчислення цього коду є проміжним технологічним етапом при формуванні ЕЦП, що накладається на ЕД. Після цього користувач формує запит на формування позначки часу, який містить, у тому числі й обчислений геш-код, і передає його до ЦСК. В свою чергу, ЦСК перевіряє правильність формату запиту та виконує його обробку, формує позначку часу та відповідь, що містить цю позначку, чи відповідь з інформацією про відмову у формуванні позначки часу.

За результатом опрацювання цієї послуги ЦСК пересилає користувачеві відповідь, що містить позначку часу, засвідчену ЕЦП центру. Сформована позначка часу, тобто сукупність електронних даних, створена за допомогою технічних засобів, містить у тому числі й геш-код ЕД (електронного набору даних), для яких було сформовано позначку, час її формування та серійний номер.

Користувач після отримання відповіді, отриманої від ЦСК, перевіряє результат обробки свого запиту у відповіді центру. За позитивного результату обробки користувачем перевіряється відповідність імені суб'єкта, що підписав позначку часу, власне імені ЦСК, наявність у центру права формувати позначки часу, чинність СВК центру та справжність ЕЦП, накладеного на отриману від центра позначку. Після цього користувач порівнює попередньо обчислений ним геш-код ЕД та геш-код, записаний у позначці часу. За позитивним результатом порівняння позначка часу може бути додана до ЕД.

Перевірка позначки часу може бути виконана будь-яким суб'єктом (верифікатором) за допомогою СВК, що належить ЦСК, автономно, без взаємодії з цим центром. З цією метою верифікатор витягує позначку часу з ЕД, до якого вона була прикріплена, і отримує з неї ідентифікаційну інформацію про ЦСК. На її основі може бути отриманий СВК, що належить ЦСК, який зберігається у ЦЗО (засвідчувальному центрі). За допомогою чинного (на момент формування позначки) СВК центру сертифікації ключів версифікатор перевіряє справжність ЕЦП, накладеного на позначку часу. Після цього, шляхом порівняння обчисленого геш-коду ЕД та геш-коду, що зберігається у позначці часу, можна вже перевірити відповідність позначки часу та ЕД, до якого вона була прикріплена.

Позначка часу на ЕД засвідчує точний час, на який цей документ вже існував і тому за її допомогою в подальшому можна буде розв'язувати конфлікти, пов'язані з використанням цього документа. Зокрема, за її допомогою можна забезпечити не відмовність автора ЕД від свого ЕЦП.

Наявність позначки часу, доданої до ЕД, дозволяє продовжувати термін дії накладеного на нього ЕЦП. Така позначка (штамп) засвідчує, наприклад, що ЕЦП був накладений на ЕД до того, як відповідний СВК був анульований (відкликаний). Таким чином, для перевірки справжності ЕЦП, накладеного на ЕД до моменту відкликання СВК, можна використовувати ВК, що міститься у вже анульованому або відкликаному сертифікаті. Ланцюжок позначок часу дозволяє створювати системи архівного зберігання ЕД, причому зі збереженням справжності ЕЦП, накладених на ці документи. В іншому випадку, справжність підписаного ЕД обмежена терміном дії СВК, який був чинним на момент накладання ЕЦП.

Слід підкреслити, що для отримання позначки часу користувач не повинен надсилати до ЦСК ні сам ЕД (електронний набір даних), ні накладений на нього ЕЦП. Тобто процедура формування позначки часу жодним чином не може порушити конфіденційність ЕД (електронного набору даних) і вона може бути використана, наприклад, як один з механізмів у підтвердженні авторства на літературний твір, аудіовізуальний твір у цифровому форматі, базу даних, комп'ютерну програму тощо.

Інфраструктура відкритого ключа

Сертифікат відкритого ключа

За умови корпоративного використання ЕЦП, тобто визначеним колом осіб, для забезпечення перевірки справжності підписів цих осіб їм достатньо обмінятися між собою ВК. Крім того, за такої ситуації питання ідентифікації особи підписувача не стоїть. Доступність і достовірність приналежності ВК може бути досягнута за допомогою певних правил, яких повинні дотримуватися зазначені особи в межах цієї корпорації.

Для забезпечення можливості перевірки справжності ЕЦП невизначеним колом осіб на практиці напрацьований механізм використання СВК, що являє собою документ, виданий ЦСК, який засвідчує чинність і належність ВК підписувачу.

Відповідно до статті 6 Закону України "Про електронний цифровий підпис" СВК містить такі обов'язкові дані:

– найменування та реквізити ЦСК (ЦЗО, засвідчувального центру);

– зазначення, що СВК виданий в Україні;

– унікальний реєстраційний номер СВК;

– основні дані (реквізити) підписувача - власника ОК;

– дату і час початку та закінчення строку чинності СВК;

– відкритий ключ;

– найменування криптографічного алгоритму, що використовується власником ОК;

– інформацію про обмеження використання ЕЦП.

При цьому ПСВК, крім обов'язкових даних, які містяться в СВК, повинен мати відповідну ознаку (що це є, власне, ПСВК).

Інші дані можуть вноситися у ПСВК на вимогу його власника.

Суб'єкти інфраструктури відкритого ключа підпису

Основу ІВК (англ. *PKI - Public Key Infrastructure*) складають суб'єкти, які є ЦСК, частина з яких має статус АЦСК. Головною функцією ЦСК є надання можливості необмеженому колу користувачів мати доступ до СВК підписувачів через загальнодоступні телекомунікаційні мережі, зокрема через Інтернет. Наявність СВК дає змогу перевірити справжність ЕЦП, накладеного підписувачем, та ідентифікувати його особу.

Ключовим елементом ІВК є ЦЗО, який визначається Кабінетом Міністрів України і веде Реєстр суб'єктів – засвідчувальних центрів та акредитованих центрів сертифікації ключів, які надають визначені Законом України "Про електронний цифровий підпис" послуги, пов'язані з ЕЦП (послуги ЕЦП). Головною функцією ЦЗО в ІВК є засвідчення приналежності ВК відповідним ЦСК, які, в свою чергу, засвідчують приналежність ВК підписувачам. Умовно кажучи, довіра до ЦЗО поширюється на СВК, що належать ЦСК, а довіра до ЦСК – відповідно на СВК підписувачів. На сьогодні функції ЦЗО виконує Міністерство юстиції України.

В інституційному забезпеченні функціонування ІВК важливу роль відіграє Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Відповідно до статті 12 зазначеного Закону функції контролюючого органу (КО) здійснює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (на сьогодні – Адміністрація Держспецзв'язку). Для забезпечення здійснення своїх функцій Адміністрація Держспецзв'язку своїм наказом затвердила "Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису", відповідно до якого КО перевіряє дотримання вимог цього Закону ЦЗО, засвідчувальними центрами та ЦСК.

Відповідно до статті 10 зазначеного Закону Кабінет Міністрів України за необхідності визначає засвідчувальний центр центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи ЦСК, які надають послуги ЕЦП цьому органу і підпорядкованим йому підприємствам, установам та організаціям. Засвідчувальний центр по відношенню до такої групи ЦСК має ті ж функції і повноваження, що й ЦЗО стосовно ЦСК. Інші

державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання таких функцій.

Згідно з частиною сьомою статті 5 зазначеного Закону порядок застосування ЕЦП в банківській діяльності визначається Національним банком України. Зокрема, Національний банк України прийняв постанову "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України ". Для забезпечення формування складової ІВК для банківської системи України та створення умов для подальшого функціонування ЕЦП в банківській діяльності Кабінет Міністрів України відповідним розпорядженням погодив створення Засвідчувального центру Національного банку України. Це, зокрема, надасть змогу досягти зменшення витрат банківської системи на послуги ЕЦП за рахунок використання централізованої інфраструктури відкритих ключів та прискорити більш широке застосування ЕЦП в банківській системі й сприяти подальшому розвитку сучасних ІТ у банківської діяльності.

Центр сертифікації ключів

За наявності ІВК будь-яка фізична або юридична особа, що виявила бажання застосовувати у своїй діяльності ЕЦП, може звернутися до ЦСК (АЦСК) або до його повноважного представника, який в ході процедури реєстрації здійснює ідентифікацію заявника і отриманих від нього даних, необхідних для формування СВК (ПСВК). При цьому ЦСК формує СВК підписувача у вигляді документа, завіреного своїм підписом. Обов'язковим елементом цього документа є ВК підписувача. Після того, як ЦСК сформував СВК, він надає його підписувачу, для якого цей СВК був сформований, а також забезпечує вільний доступ користувачів до цього документа через загальнодоступні телекомунікаційні канали у разі згоди на це підписувача.

Відповідно до статті 6 Закону України "Про електронний цифровий підпис" ЦСК може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги ЕЦП та засвідчила свій ВК у ЦЗО або засвідчувальному центрі з дотриманням вимог статті 6 зазначеного Закону. Обслуговування фізичних та юридичних осіб здійснюється ЦСК на договірних засадах.

Відповідно до цього Закону послугами ЕЦП є:

– надання у користування засобів ЕЦП;

– допомога при генерації ВК та ОК;

– обслуговування СВК (формування, розповсюдження, скасування, зберігання, блокування та поновлення);

– надання інформації щодо чинних, скасованих і блокованих СВК;

– послуги фіксування часу;

– консультації та інші послуги.

Акредитований центр сертифікації ключів

Відповідно до статті 9 Закону України "Про електронний цифровий підпис" ЦСК, акредитований в установленому порядку, є АЦСК. Процедура акредитації, яка здійснюється на добровільних засадах, документально засвідчує компетентність ЦСК здійснювати діяльність, пов'язану з обслуговуванням ПСВК. При цьому АЦСК має виконувати усі зобов'язання та вимоги, встановлені законодавством для ЦСК, та додатково зобов'язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП.

Відповідно до "Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" установа, тобто будь-який суб'єкт, зазначений в цьому Порядку, отримує на договірних засадах послуги ЕЦП від АЦСК. При цьому установа може отримувати такі послуги лише від одного АЦСК, а використання підписувачами (працівниками установи) ОК, відповідні ВК яких засвідчені іншими АЦСК, забороняється.

На виконання постанови Кабінету Міністрів України "Про затвердження Порядку акредитації центру сертифікації ключів" наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (його правонаступником є Адміністрація Держспецзв'язку) затверджено "Правила посиленої сертифікації", які визначають організаційні, технічні і технологічні вимоги до АЦСК під час обслуговування ними ПСВК та забезпечення їх використання. Відповідно до зазначеного Порядку та з метою створення умов технологічної сумісності програмно-технічних комплексів АЦСК та засобів ЕЦП спільним наказом

Держкомінформнауки та Держспецзв'язку були затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису", що містять:

– формат підписаних даних;

– протокол фіксування часу;

– протокол визначення статусу ПСВК.

Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмно-технічних комплексів АЦСК. Правильність реалізації наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері КЗІ. Тип формату ЕЦП обирається залежно від вимог до зберігання підписаних даних.

Розповсюдження сертифікатів відкритих ключів

Згідно із законодавством СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. При цьому ПСВК є СВК, який відповідає вимогам Закону України "Про електронний цифровий підпис", виданий АЦСК, засвідчувальним центром, ЦЗО. Відповідно до статті 8 цього Закону ЦСК зобов'язаний забезпечувати цілодобово доступ користувачів до СВК та відповідних електронних переліків СВК через загальнодоступні телекомунікаційні канали.

Користувачі у разі необхідності отримують СВК підписувача з бази даних сертифікатів ЦСК і при цьому перевіряється статус цього СВК (чинний, заблокований, скасований). Перевірка ЕЦП може здійснюватися за допомогою ВК, що міститься у СВК, лише у разі, коли на цей момент сертифікат є чинним (рис. 3).

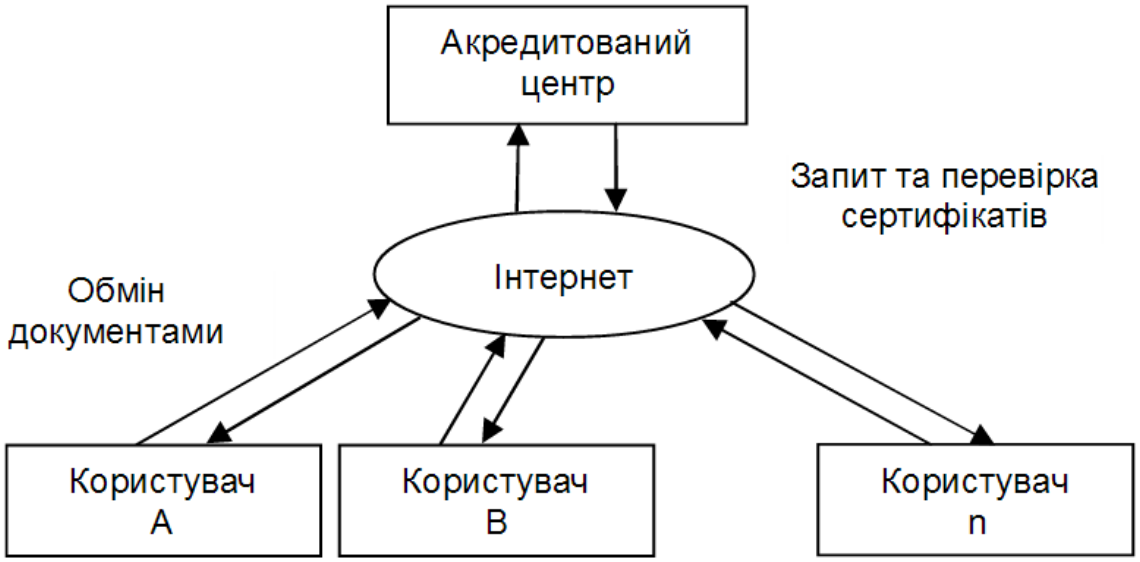

Рис. 3. ***Схема взаємодії користувачів електронного цифрового підпису***

Обов'язкова передача документованої інформації центрів сертифікації ключів

Сукупність СВК, які зберігаються АЦСК, відповідні реєстри, та інша документована інформація є головною інформаційною складовою ІВК. За її неповноти коло суб'єктів, що застосовують ЕЦП, буде обмеженим і може звестися лише до корпоративних груп, які самостійно будуть обмінюватися між собою ВК. Для забезпечення захисту прав суб'єктів, які використовують ЕЦП, та стабільного існування ІВК необхідно створити юридичні та організаційні умови, за яких гарантовано буде збережено зазначену інформацію.

Відповідно до статті 14 Закону України "Про електронний цифровий підпис" ЦСК припиняє свою діяльність відповідно до законодавства. Про рішення щодо припинення своєї діяльності ЦСК повідомляє підписувачів за три місяці, якщо інші строки не визначено законодавством. При цьому АЦСК додатково повідомляє про рішення щодо припинення діяльності ЦЗО або відповідний засвідчувальний центр і протягом доби, визначеної як дата припинення його діяльності, відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку обов'язкової передачі документованої інформації" передає ПСВК, відповідні реєстри ПСВК та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або ЦЗО.

ТЕМА Основні поняття криптології. Криптографічні методи захисту інформації

Криптологія – наука про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й крипто аналіз. Слід зазначити, що ці дві науки – парна категорія. Розвиток однієї з них є поштовхом для іншої. Розглядати окремо криптографію від крипто аналізу, значить порушити основи філософії й один з її законів єдності й боротьби протилежностей.

Криптографія – займається пошуком і дослідженням методів перетворення інформації з метою приховання її змісту. Основні напрямки використання криптографічних методів - передача конфіденційної інформації з каналів зв'язку, установлення дійсності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому виді.

Крипто аналіз – дослідження можливості розшифровування інформації без знання ключів. У якості інформації, що підлягає шифруванню й розшифровуванню, будуть розглядатися тексти, побудовані на деякому алфавіті. Під цими термінами розуміється наступне.

Алфавіт — кінцева множина використовуваних для кодування інформації знаків. Слід зазначити той факт, що в якості алфавіту можуть виступати як множина символів національних алфавітів, так і множина різних символів (наприклад, танцюючих чоловічків) і цифр.

Текст — упорядкований набір з елементів алфавіту.

Шифрування - процес перетворення вихідного тексту, який носить також назву відкритого тексту, у шифрований текст.

Розшифрування – процес, зворотний шифруванню. На основі ключа шифрований текст перетвориться у вихідний.

Ключ - цей конкретний секретний стан деяких параметрів алгоритму криптографічного перетворення даних, що забезпечує вибір тільки одного варіанта з усіх можливих для даного алгоритму. Звичайно ключ являє собою послідовний ряд символів алфавіту.

Простір ключів —це набір можливих значень ключа.

Криптографічна система – являє собою сімейство *T* перетворень відкритого тексту.

У симетричних криптосистемах для шифрування й для розшифровування використовується один і той самий ключ.

У системах з відкритим ключем використовуються два ключі-відкритий і закритий (секретний*),* які математично зв'язано один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачеві повідомлення.

Терміни «розподіл ключів» і «керування ключами» ставляться до процесів системи обробки інформації, змістом яких є вироблення й розподіл ключів між користувачами.

Електронним цифровим підписом називається його криптографічне перетворення, що приєднується до тексту, яке дозволяє при одержанні тексту іншим користувачем перевірити авторство й дійсність повідомлення.

Криптологічною стійкістю називається характеристика шифру, що визначає його стійкість до розшифровування без знання ключа (тобто крипто аналізу). Є кілька показників крипто стійкості, серед яких:

- кількість усіх можливих ключів;
- середній час, необхідний для успішної крипто аналітичної атаки того або іншого виду.

Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа й крипто стійкості шифру.

2. Вимоги до криптографічних систем

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, однак їй властиві й переваги: висока продуктивність, простота, захищеність. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

- зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення;
- знання алгоритму шифрування не повинно впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту;
- незначна зміна вихідного тексту повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення у процесі шифрування, повинні бути повністю й надійно сховані у шифрованому тексті;
- довжина шифрованого тексту не повинна перевершувати довжину вихідного тексту;
- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
- будь-який ключ із множини можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Не слід забувати й про такі банальні речі, як гроші. Іншими словами - скільки буде коштувати збиток, який понесе власник інформації, при несанкціонованім її

використанні? чи коштує ця інформація тих вкладень, які необхідно зробити для закриття інформації?

3 Основні положення та визначення криптографії

Проблемою захисту інформації шляхом її перетворення займається **криптологія** (kryptos - таємний, logos - повідомлення). Вона має два напрямки: **криптографію і крипто аналіз**. Цілі цих двох напрямків прямо протилежні.

Криптографія займається пошуком, дослідженням і розробкою математичних методів перетворення інформації, основою яких є шифрування, а **крипто аналіз** - дослідженням можливості роз шифровки інформації.

Основні напрямки використання криптографічних методів - це передача конфіденційної інформації через канали зв'язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, збереження інформації (документів, баз даних) на носіях у зашифрованому виді.

Сучасна криптографія вивчає і розвиває такі напрямки:

- симетричні крипто системи (із секретним ключем);
- несиметричні крипто системи (з відкритим ключем);
- системи електронного підпису;
- системи керування ключами.

Сучасні криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа. Однак, на практиці будь-який шифр, який використовується в тій або іншій крипто системі, піддається розкриттю з визначеною трудомісткістю. У зв'язку з цим, виникає необхідність оцінки крипто стійкості шифрів, які застосовуються, в алгоритмах крипто перетворення.

Допомагаючи зберегти зміст повідомлення в таємниці, **криптографію можна використовувати для забезпечення:**

- автентифікації;
- цілісності;
- незаперечності.

При автентифікації одержувачеві повідомлення потрібно переконатися, що воно виходить від конкретного відправника. Зловмисник не може надіслати фальшиве повідомлення від будь-якого імені.

При визначенні цілісності одержувач повідомлення в змозі перевірити, чи були внесені які-небудь зміни в отримане повідомлення під час його передачі. Зловмисникові не дозволено замінювати дійсне повідомлення на фальшиве.

Незаперечність необхідна для того, щоб відправник повідомлення не зміг згодом заперечувати, що він не є автором цього повідомлення.

В даний час **автентифікація**, що здійснюється користувачем, забезпечується за допомогою:

- смарт-карт;
- засобів біометрії;
- клавіатури комп'ютера;
- криптографії з унікальними ключами для кожного користувача.

Основною областю застосування смарт-карт є ідентифікація користувачів мобільними телефонами.

Біометрія заснована на анатомічній унікальності кожної людини. Біометричні системи ідентифікації приведені на рис. 3.1.

Рис. 3.1 Біометричні системи ідентифікації

Цілісність інформації забезпечується за допомогою криптографічних контрольних сум і механізмів керування доступом і привілеями. У якості криптографічної контрольної суми для виявлення навмисної або випадкової модифікації даних використовується код автентифікації повідомлення - MAC (Message Autentification Code).

Для виявлення **несанкціонованих** змін у переданих повідомленнях можна застосувати:

- електронно-цифровий підпис (ЕЦП), заснований на криптографії з відкритим і закритим ключами;
- програми виявлення вірусів;
- призначення відповідних прав користувачам для керування доступом;
- точне виконання прийнятого механізму привілеїв.

Незаперечність – повідомлення підтверджується електронно-цифровим підписом.

4. Характеристика алгоритмів шифрування

В даний час спостерігається різке зростання об’ємів інформації (у тому числі і конфіденційної), яка передається по відкритих каналах зв'язку. Тому все більш актуальнішою стає проблема захисту переданої інформації. Незважаючи на те, що конкретні реалізації систем захисту інформації можуть істотно відрізнятися одна від одної через розходження методів і алгоритмів передачі даних, усі вони повинні забезпечувати **рішення триєдиної задачі:**

- конфіденційність інформації (доступність її тільки для того, кому вона призначена);
- цілісність інформації (її достовірність і точність, а також захищеність від навмисних і ненавмисних перекручувань);
- готовність інформації (використання в будь-який момент, коли в ній виникає необхідність).

Успішне рішення перерахованих задач можливе як за рахунок використання **організаційно-технічних заходів**, так і за допомогою **криптографічного захисту інформації.**

Організаційно-технічні заходи містять у собі фізичну охорону об'єктів конфіденційної інформації, застосування спеціального адміністративного персоналу і цілий ряд інших дорогих технічних заходів для захисту важливих даних.

Криптографічний захист у більшості випадків є більш ефективним і дешевим. Конфіденційність інформації при цьому забезпечується шифруванням переданих документів або всього трафіка.

Процес криптографічного захисту даних може здійснюватися як **програмно**, так і **апаратно**. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги це - висока продуктивність, простота, захищеність. Програмна реалізація більш практична, допускає значну гнучкість у використанні. **Перед сучасними криптографічними системами захисту інформації ставлять наступні вимоги:**

- зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинно мати чітку нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);
- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення у процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;
- довжина шифрованого тексту повинна бути рівна довжині вихідного тексту;
- не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;

- будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Сам по собі криптографічний алгоритм, названий **алгоритмом шифрування,** являє собою деяку математичну функцію, яка використовується для шифрування і роз шифровки. Точніше таких функцій дві: одна застосовується для шифрування, а інша - для роз шифрування.

Розрізняється шифрування двох типів:

- симетричне (із секретним ключем);
- несиметричне (з відкритим ключем).

При симетричному шифруванні (рис.3.2) створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв'язку. Адресат, запустивши ту ж саму шифрувальну програму з отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.

Рис. 3.2 Симетричне шифрування

Несиметричне шифрування складніше, але і надійніше. Для його реалізації (рис. 3.2) потрібні два взаємозалежних ключі: відкритий і закритий. Одержувач повідомляє всім бажаючим свій відкритий ключ, що дозволяє шифрувати для нього

повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифроване повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. За підвищену надійність несиметричного шифрування приходиться платити: оскільки обчислення в цьому випадку складніше, то процедура роз шифровки займає більше часу.

Коли надійність криптографічного алгоритму забезпечується за рахунок збереження в таємниці суті самого алгоритму, такий алгоритм шифрування називається **обмеженим.** Обмежені алгоритми становлять значний інтерес з погляду історії криптографії, однак зовсім непридатні при сучасних вимогах, які висуваються до шифрування. Адже, в цьому випадку, кожна група користувачів, які бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми шифрування.

Рис. 3.3 Несиметричне шифрування

У сучасній криптографії зазначені вище проблеми вирішуються за допомогою використання ключа, який потрібно вибирати серед значень, що належать безлічі (ключовий простір). Функції шифрування і розшифрування залежать від цього ключа. Деякі алгоритми шифрування використовують різні ключі для шифрування і розшифровування. Це означає, що ключ шифрування відрізняється від ключа розшифровування.

Надійність алгоритму шифрування з використанням ключів досягається за рахунок їх належного вибору і наступного збереження в найсуворішому секреті. Це означає, що такий алгоритм не потрібно тримати в таємниці. Можна організувати масове виробництво криптографічних засобів, в основу функціонування яких

покладений даний алгоритм. Навіть знаючи криптографічний алгоритм, зловмисник не зможе прочитати зашифровані повідомлення, оскільки він не знає секретний ключ, використаний для його зашифровування.

Симетричні алгоритми шифрування поділяються на:

- потокові;
- блокові.

Алгоритми, у яких відкритий текст обробляється побітно, називаються **потоковими алгоритмами** або **потоковими шифрами.** В інших алгоритмах відкритий текст розбивається на блоки, що складаються з декількох біт. Такі алгоритми називаються **блоковими** або **блоковими шифрами.**

Симетричні алгоритми при виявленні в них яких-небудь слабкостей можуть бути дороблені шляхом внесення невеликих змін, а для несиметричних - така можливість відсутня.

Симетричні алгоритми працюють значно швидше, ніж алгоритми з відкритим ключем. На практиці несиметричні алгоритми шифрування часто застосовуються в сукупності з симетричними алгоритмами: відкритий текст зашифровується симетричним алгоритмом, а секретний ключ цього симетричного алгоритму зашифровується на відкритому ключі несиметричного алгоритму. Такий механізм називають **цифровим конвертом** (digital envelope). Найширше в даний час застосовуються наступні алгоритми шифрування:

- DES (Data Encryption Standard);
- Blowfish;
- IDEA (International Decryption-Encryption Algorithm);
- ГОСТ 28147-89;
- RSA (автори: Rivest, Shamir і Alderman);
- PGP.

У симетричних крипто алгоритмах (DES, ДСТ, Blowfish, RC5, IDEA) для шифрування і розшифрування інформації використовується той самий секретний ключ. Перевагами таких алгоритмів є:

- простота програмної та апаратної реалізації;
- висока швидкість роботи в прямому і зворотному напрямках;

- забезпечення необхідного рівня захисту інформації при використанні коротких ключів.

До основних недоліків цих крипто алгоритмів варто віднести збільшення витрат по забезпеченню додаткових заходів таємності при поширенні ключів, а також те, що алгоритм із секретним ключем виконує свою задачу тільки в умовах повної довіри кореспондентів один одному.

У несиметричних крипто алгоритмах (RSA, PGP, ECC) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв'язку, що дозволяє по одному ключу обчислити інший. За допомогою відкритого ключа практично будь-який користувач може зашифрувати своє повідомлення або перевірити електронно-цифровий підпис. Розшифрувати таке повідомлення або поставити підпис може тільки власник секретного ключа.

Такі алгоритми дозволяють реалізувати протоколи типу цифрового підпису, забезпечують відкрите поширення ключів і надійну автентифікацію в мережі, стійку навіть до повного перехоплення трафіка.