замінені на їхні порядкові номери, які розглядаються за модулем 23 (mod 23),так як в латинському алфавіті 23 літери. Ця ідея заміни символів на відрахування вельми корисна і застосовується в сучасних криптосистемах. Узагальненням системи Цезаря служить Афінна криптосистема. Розглянемо шифрування англійських текстів за допомогою наступного методу. Зіставивши кожній букві англійського алфавіту лишок за модулем 26.Обиремо два числа k и m ($1 \le k \le 25$; $0 \le m \le 25$), причому НОД (k,26)=1.Шифруємо так: лишок замінюється на лишок. Враховуючи, які різні значення можна надати k і m, отримуємо 312 способів шифрування англійських текстів. Однозначно дешифрувати повідомлення можна, якщо відомі k і m (зворотний лишок до лишка).

Висновки. Розглядаючи теорію лишків і кодування можна побачити, що цей розділ математики посідав й посідає дуже важливе місце у житті людини, як в минулому, так і зараз, бо секретність будь-якої важливої інформації можливо зберегти лише за допомогою кодування або шифрування її. Ще не варто забувати, що один з найважливіших винаходів людини - комп`ютер, працює саме через постійне кодування.

Список використаних джерел

1. Берман Г.Н. Число и наука про него / Г.Н. Берман. - М. Государственное издательство технико-теоретической литературы, 1954.-157 с.
2. Илларионова О.Г., Солодов В.В. Комплексные числа, алгебраические структуры / О.Г. Илларионова, В.В.Солодов - М.: МГТУ ГА, 2005. - 24 с.

УДК 004.056.55(043.2)

Мосєвніна А.С.,
здобувач вищої освіти,
Половенко Л.П., доцент, доцент
кафедри прикладної математики

ЕЛЕКТРОННИЙ ПІДПИС: БЕЗПЕКА ТА ЗАХИЩЕНІСТЬ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

В Україні широкого поширення набуло використання електронних документів. Вони не лише існують поряд з традиційними паперовими документами, але все частіше замінюють їх. Цьому сприяють наростаючий темп розвитку цифрових технологій та впровадження на державному рівні проєктів у сфері цифрової трансформації. Легітимним засобом електронної ідентифікації виступає електронний цифровий підпис (ЕЦП). Застосування ЕЦП дозволяє суттєво економити час, необхідний на оформлення

документації, забезпечуючи при цьому цілісність інформації. та підтвердження автентичності власника ключа.

Основні тенденції розвитку та використання електронних цифрових підписів висвітлено у працях У. З. Ватаманюк-Зелінської, В. С. Сушко та ін. Проблему захисту особистих ключів користувачів порушують С. Лур'є, Л. В. Піддубна, В. М. Павліченко та ін. Проте недостатньо висвітлено питання оптимального вибору типу електронного підпису з точки зору надійності та ефективності використання водночас.

Електронний цифровий підпис – це дані в електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів. ЕЦП виконує безпековий аспект щодо інформації, яку він містить, також підтверджує автентичність власника ключа, який можна отримати в спеціалізованих центрах сертифікації ключів. Сертифікат відповідає за достовірність даних власника і містить відкритий ключ, підтверджений підписом довіреної особи. ЕЦП майже неможливо підробити. Така система дає змогу захистити ключ від підміни, а отже може бути затверджена на законодавчому рівні. [1] Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу в Державній службі спеціального зв'язку та захисту інформації України. Послуги з надання ЕЦП в Україні впроваджуються акредитованими центрами сертифікації ключів [2].

За допомогою послуг ЕЦП можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Підписані таким чином документи мають таку саму юридичну силу, як і звичайні. Підприємства, компанії, установи переходять на програмні рішення електронного підпису, оскільки це дозволяє суттєво зменшити споживання паперу, скоротити витрати та підвищити ефективність документообміну.

Неможливість підробки електронного цифрового підпису забезпечується дуже великим обсягом математичних обчислень, необхідних для його підбору. Таким чином, при отриманні документу, підписаного електронним цифровим підписом, одержувач може бути впевнений в авторстві і незмінності тексту даного документа.

Проте користуючись ЕЦП не варто нехтувати безпекою. В контексті безпечного використання ЕЦП С Лур'є зосереджує увагу на захисті особистих (таємних) ключів користувачів [5]. Оскільки заволодівши чужим ключем, зловмисник потенційно зможе від імені жертви накладати електронний цифровий підпис на документах та вчиняти дії в інформаційних системах, змінювати записи в базах даних, проводити нелегітимні грошові транзакції, розшифрувати зашифровану для жертви інформацію тощо.

За рівнем довіри розрізняють три типи електронних підписів:

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

Тільки останній вид ЕЦП – кваліфікований з високим рівнем довіри відповідає власноручному підпису.

ЕЦП використовують наступні засоби:

- файлові, які зберігаються на комп'ютері чи звичайних флешках, тощо;
- підписи, які зберігаються на захищених носіях - токени або хмарні сервіси;
- підписи, які зберігаються на SIM-карті мобільного телефона - Mobile ID.

Файлові підписи можна копіювати і зберігати у будь-якому місці, а токени, хмарні сховища і Mobile ID не підлягають копіюванню, тому є більш надійними, як свідчить Міжнародна практика використання засобів ЕЦП. При використанні захищених носіїв підвищується безпека даних та довіра до електронних підписів.

Токен потрібно під'єднати до комп'ютера та зчитати, а при використанні Mobile ID - ввести номер телефону та персональний пін-код, створений при підключенні послуги Mobile ID. До ключа в хмарному сховищі у власника є доступ з будь-якого пристрою з виходом в Інтернет [5].

Захищений носій особистих ключів має вбудовані апаратно-програмні засоби, що забезпечують захист даних від несанкціонованого доступу, зокрема, від ознайомлення із значенням параметрів особистих ключів та їх копіювання. В ньому відбувається створення (генерація), зберігання та використання ключів. Діє він за принципом «чорного ящика», тобто можливості отримати ззовні доступ до внутрішніх процесів неможливо.

На відміну від використання інших видів носіїв, ключ не створюється, не зберігається і не використовується на робочому комп’ютері в оперативній пам’яті, саме тому викрасти його звідти також неможливо. Викрадення ключа можливе лише разом з носієм, проте непомітним для власника ключа це вже не залишиться. Власник відразу може звернутися до центру сертифікації ключів і заблокувати сертифікат такого ключа. Натомість, ключі, згенеровані на незахищених носіях, можуть бути викрадені шляхом простого копіювання або за допомогою шкідливого програмного забезпечення без залишення слідів такого викрадення.

Використання захищених носіїв — це необхідний засіб захисту своїх інтересів його власником при використанні ЕЦП. Розглянемо більш детально засоби збереження ключів.

Токен – спеціальний USB-пристрій у формі смарт-картки (картки з чипом) або флешки, на якому зберігаються особисті ключі ЕЦП та

інформація щодо власника, який затверджений Держслужбою спецзв'язку і має унікальний інвентарний номер. Прикладами токенів є пристрої Алмаз-1К, Кристал-1, Гряда-301 тощо.

Електронний підпис можна отримати на ID-картці. Особисті ключі ЕЦП зберігаються на безконтактному електронному носії – чіпі. Підпис на ID-карті неможливо скопіювати на флешку чи інший електронний носій.

Захищене хмарне сховище – це програмно-апаратний комплекс, завдяки якому можна зберігати інформацію у депозитарії, що створений згідно норм чинного законодавства у сфері захисту інформації та електронних довірчих послуг. Воно дає можливість віддалено зберігати, керувати і використовувати особисті ключі ЕЦП.

DepositSign – інноваційний сервіс, який також дозволяє зберігати особисті ключі електронного цифрового підпису у депозитарії. Перевагами зберігання ключів ЕЦП в такому сховищі є безумовна захищеність, ключ неможливо втратити, загубити чи видалити. Є двофакторна авторизація. Також DepositSign надає електронну довірчу послугу – послуга, яка забезпечує електронну взаємодію двох або більше суб'єктів. DepositSign дозволяє отримати і використовувати будь-яку кількість КЕП всередині компанії, інтегрувати функціонал DepositSign до сервісів, web-сайтів та додатків для здійснення юридично значущих операцій, забезпечує повний контроль над використанням ключів співробітниками включно із відкликанням доступу.

CloudKey – хмарний носій, завдяки якому можна зберігати особисті ключі ЕЦП у провайдера ТОВ «ЦСК «Україна» всередині захищеного апаратно-програмного пристрою. Для послуги CloudKey використовує мережевий криптомодуль ІІТ Гряда-301. Після успішної аутентифікації доступ до ключа в криптомодулі є лише у власника. Ефективний для підписання та подання звітності ФОПів та юридичних осіб; для обміну юридично важливими електронними документами; для підписання чеків у ПРРО; для авторизації на порталах надання державних послуг. Перевагами CloudKey є постійний доступ до ключів, відсутній ризик втрати ключа, наявність комплексної системи захисту інформації, яка пройшла державну експертизу і має атестат відповідності.

Дія.Підпис – це кваліфікований електронний підпис для підписання документів. Його можна згенерувати в застосунку Дія. Якщо ЕЦП Дія.Підпис був створений на одному ґаджеті, то скористатися ним з іншого не можна. Тому треба буде авторизуватися у застосунку Дія на новому ґаджеті і створити новий ЕЦП. При цьому минулий електронний підпис автоматично видаляється.

SmartID – це кваліфікований електронний цифровий підпис, який є аналогом власноручного підпису. Завдяки SmartID можна підписувати документи, звіти, платежі і отримувати послуги онлайн. Підпис SmartID

зберігається в захищеному хмарному сховищі, яке відповідає вимогам Закону України № 2155 «Про електронні довірчі послуги». Отримати доступ до свого підпису SmartID можна з будь-якого смартфону, на який встановлено додаток «Приват24 для бізнесу». SmartID неможливо загубити, забути чи скомпрометувати.

Кваліфікований надавач електронних довірчих послуг ТОВ «Вчасно» забезпечує при покупці ключа «Вчасно.КЕП», можливість отримати «комплект ключів». Тобто, купуючи апаратний (токен) або хмарний ключ, можна створити заявку на отримання файлового ключа, який вам нададуть як бонус. Недоліком є те, що отримати ключ дистанційно неможливо, оскільки згідно з законом особиста присутність заявника є обов'язковою.

Mobile ID – це технологія для запису і зберігання КЕПу на SIM-карті. Також дозволяє занести іншу персональну інформацію про людину на SIM-карту: ідентифікаційний код, паспортні дані тощо. Перевагами Mobile ID є висока захищеність особистих даних. Оскільки внесена інформація закодована і захищена паролями, то її неможливо видалити або скопіювати. У випадку втрати телефону інша особа не зможе використати ваш ЕЦП [3].

В процесі прийняття рішення щодо застосовування захищених носіїв для зберігання сертифікатів підпису слід враховувати як це впливає на безпеку з одного боку і на швидкість та сталість внутрішніх процесів з іншого. Якщо, наприклад, ключ потрібний лише для роботи в локальних системах електронного документообігу, то можна використовувати Mobile ID, флешку або хмарний сервіс, коли багато співробітників. А якщо в будь-яких системах, в тому числі державних, то краще хмару або токени (захищена флешка). Також варто використовувати захищені носії для підписання критично важливих документів. Це мінімізує шанси визнання їх недійсними в разі можливих судових суперечок.

Вибір рішення також залежить від обсягу документообігу. Якщо потрібно лише декілька разів на рік щось підписати, то достатньо Mobile ID, а якщо тисячі документів на день, то без хмарних сервісів буде вже важко. Якщо компанія має понад 100 співробітників, то краще скористатися послугами провайдерів хмарних сховищ. Якщо працівник звільнився або у відпустці, то ключ на флешці або токен у такому випадку неможливо контролювати. А хмарні сервіси дають можливість бачити всі транзакції, які відбуваються з підписами, і забороняти доступ до ключа в залежності від того, де і коли знаходиться співробітник. Це і посилює контроль, і підвищує рівень безпеки інформації.

Список використаних джерел

1. *Ватаманюк-Зелінська У. З., Сушко В. С. Перспективи використання електронного цифрового підпису в державних структурах. Ефективна економіка. URL: http://www.economy.nayka.com.ua/pdf/7_2020/12.pdf*

2. *Що таке електронний цифровий підпис? [Урядовий портал]. URL: https://www.kmu.gov.ua/usi-pitannya-po-e-poslugam/sho-tak-elektronnij-cifrovij-pidpis-ecp*
3. *ЕЦП або КЕП: чим підписувати електронні документи? URL: https://biz.ligazakon.net/analitycs/200366_etsp-abo-kep-chim-pdpisuvati-elektronn-dokumenti*
4. *Піддубна Л. В., Павліченко В. М., Інформаційна безпека в системах електронного документообігу. Науковий вісник Полтавського університету економіки і торгівлі. 2019. № 4 (95) http://journal.puet.edu.ua/index.php/nven/article/viewFile/1588/1422*
5. *Станісла Лур'є. Безпечність використання електронного цифрового підпису URL: https://investgazeta.ua/blogs/bezpechnist-vikoristannya-elektronnogo-tsifrovogo-pidpisu*

УДК 546.07

Сохацький Ф.М., д.ф.-м.н., доцент, доцент кафедри прикладної математики
Луценко А.В., асистент кафедри прикладної математики

МАТРИЧНІ IP-КВАЗІГРУПИ 4-ГО ПОРЯДКУ

Донецький національний університет імені Василя Стуса, м. Вінниця

Центральні квазігрупи в класі квазігруп відіграють таку ж саму роль, що і комутативні групи в класі всіх груп. Крім того, центральні квазігрупи є лінійними ізотопами комутативних груп, що дозволяє значно поглибити результати про оборотність, сформульовані авторами в [2, 3], зокрема, стосовно ізотопів груп, отриманих у [4]. Матричні квазігрупи є одним із видів центральних квазігруп, а в деяких випадках збігаються з матричними квазігрупами. Тому вивчення центральних і матричних квазігруп викликає значний інтерес.

Означення 1 [1]. *Квазігрупою* називається групоїд $(Q;\cdot)$ такий, що для довільних a,b кожне з рівнянь $a\cdot x=b$, $y\cdot a=b$ має єдиний розв'язок.

Квазігруповою (оборотною) операцією називають функцію, визначену на скінченній чи нескінченній множині, якщо вона оборотна за кожною своєю змінною.

Нехай K - довільне комутативне кільце з одиницею і $K^n=K\times\ldots\times K$. Групоїд $(K^n;f)$ визначений рівністю

$$f(\bar{x},\bar{y})=\bar{x}A+\bar{y}B+\bar{a},$$

де A, $B\in M_n(K)$ і $\bar{a}\in K^n$ називається *матричною квазігрупою* над