ПРОБЛЕМНІ ПИТАННЯ ТА ОСНОВНІ НАПРЯМИ УДОСКОНАЛЕННЯ ТА РОЗВИТКУ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ ВІДКРИТОГО КЛЮЧА

Горбенко Ю.І.[1],Чичмар С.В.[1], Тоцький О.С., Бондаренко В.І.[2], Горбенко І.Д.[3]
[1]АТ «Інститут інформаційних технологій»
[2]Адміністрація Держспецзвязку
[3]Харківський національний університет радіоелектроніки
61166, Харків, вул. Бакуліна, 12, ЗАТ»ІІТ», тел.(057) 714-22-05
E-mail: GorbenkoI@iit.kharkov.ua

An analysis of the development and use of public key infrastructure in Ukraine, are considered key issues for improvement and standardization of various applications, substantiated requirements for public key certification policies and perspective cryptographic conversions.

Загально визнаним та безумовним є той факт, що стан розвитку земної цивілізації в суттєвій мірі визначається станом розвитку та застосування інформаційних технологій та інформаційно – телекомунікаційних систем в різних сферах нашого буття, здійснення стосунків в межах земної цивілізації. Зважаючи на вказане в Україні значна увага приділяється створенню та розвитку різноманітних інформаційних технологій.

Прийнята науково – технічна програма впровадження і застосування грід - технологій на 2009-2013 роки. За задумкою національний грід – являє собою просторово-розподілена обчислювальну систему, яка на даний час уже складається з більше ніж 30 обчислювальних кластерів. Грід система може працювати як єдиний потужний комп'ютер і дозволяє розв'язувати наукові і науково-технічні задачі, що потребують надвеликих обчислювальних ресурсів.

Широкого розповсюдження набуло використання специфічно поданої інформації – електронних документів і здійснення на їх основі електронного документообігу[1-4]. Уже перші впровадження підтверджують, що електронний документообіг є найбільш результативним підходом до суттєвого підвищення ефективності в різних сферах нашого буття. Надзвичайно важливим є впровадження електронного документообігу в час розбудови інформаційного суспільства, функціонування технологій електронного управління для забезпечення прозорості відносин «громадянин – держава», «підприємство – держава» та високої якості надання ***державних, комерційних і банківських послуг***.

При інтеграції в Європейський Союз для України дуже актуальними є задачі створення та розвитку національної системи біометричної верифікації і ідентифікації громадян, а також систем виготовлення та обігу ICAO – сумісних на міжнародному рівні електронних документів, включаючи електронні біометричні паспорти.

При функціонуванні вказаних систем через доступ до інформаційних ресурсів здійснюється обробка інформації систем. Під обробкою інформації в системі розуміють виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Достатньо великий досвід застосування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем і різноманітних технологій підтверджує, що в них користувачам і власникам інформації та ресурсів послуги із забезпечення безпеки інформації, що обробляється, повинні надаватись з необхідною якістю. У подальшому під послугами криптографічної системи будемо розуміти послуги цілісності, автентичності (справжності), неспростовності (спостережливості), доступності, конфіденційності та надійності тощо. В суттєвій мірі якість надання вказаних послуг визначається інфраструктурою відкритих ключів (ІВК), тобто використанням асиметричних криптографічних перетворень та криптографічних протоколів, що на них засновуються..

1. Проблемні питання застосування асиметричних криптоперетворень

Серед особливо проблемних питань сьогодні необхідно виділити наступні[4-7] : 1) стандартизація та уніфікація криптографічних примітивів, криптографічних механізмів і

протоколів; 2) узгоджене стандартизоване впровадження ІВК в грід – системи, електронний документообіг, банківські платіжні та комерційні системи, різного призначення інформаційно – комунікаційні системи тощо; 3) подальше теоретичне обґрунтування вимог та умов надання користувачам послуг ІВК з різними рівнями гарантій, та уніфікації; 4) удосконалення та розробка нових методів, механізмів та алгоритмів криптографічних перетворень по критеріям стійкості та складності; 5) прогнозування розвитку, стандартизації, уніфікації та удосконалення міжнародних ІВК; 6) практичне створення та впровадження програмно – технічних комплексів ІВК для основних призначень та уніфікованих; 7) затвердження та введення в дію основних технічних специфікацій відносно форматів даних та протоколів взаємодії тощо.

Найбільшою особливістю асиметричних перетворень є використання асиметричної пари ключів, які містить відкритий ключ,що відомий всім, та особистого ключа, що пов'язаний з відкритим ключем за допомогою певного математичного перетворення. При цьому вважається що обчислення особистого ключа, при знанні загальносистемних параметрів та відкритого ключа, повинно мати в гіршому випадку субекспоненційну складність, за умови коли обчислення відкритого ключа при формуванні асиметричної ключової пари – поліноміальну. У таблиці 1 наведені основні криптографічні перетворення для електронного цифрового підпису(ЕЦП)[5]. У таблиці 2 наведено основні асиметричні крипто перетворення, що застосовуються або можуть застосовуватись для таких криптографічних перетворень як направлене шифрування, , узгодження ключів тощо .

Таблиця 1 - Асиметричні криптографічні перетворення для ЕЦП

Парам-ри перетв-ня / Вид перетв-ня	Особистий ключ	Відкритий ключ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри	Сертифікати	Складність крипто аналізу
Перетворення в кільці (RSA)	Di	Ei	(Ei, Di)	N = PQ	Ei	Субекспоненційна
Перетворення в полі Галуа F(P) (DSA)	Xi	$Yi= g^{Xi}(\text{mod } P)$	(Xi, Yi)	P, q, g	Yi	Субекспоненційна
Перетворення в групі точок еліптичних кривих E(F(q))	di	Qi= diG(modq)	(di, Qi)	a, b, G, n, f(x)(P), h	Qi	Експоненційна
Перетворення в гіпереліптичних кривих	C_i	$D_2= c_iD1$	(ci, D2)	f(x), g(x), q, D1, g, J	D_2	Експоненційна
Перетворення зі спарюванням точок еліптичних кривих	Di = s Q_{iD}	Q_{iD} = H1(ID)	(d_{iD}, Q_{iD})	G1, G2, e, H1, P, H2, H3, F^{2m}, Pp	Q_{iD}	Міжекспоненційна – субекспоненційна

Таблиця 2 - Асиметричні криптографічні перетворення для реалізації направленого шифрування.

Параметри НШ/ Математичний апарат	Особистий ключ НРШ	Відкритий ключ НЗШ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри крипто перетворення	Сертифікати	Складність крипто аналізу
НШ в кільці (RSA)	D_i	E_i	(D_i , E_i)	$N = P\ Q$	E_i	Субекспоненційна
НШ в полі Галуа$F(P)$	X_i	$Y_i=g^X{}_i(\mathrm{mod}\ P)$	(X_i, Y_i)	P, q, g	Y_i	Субекспоненційна
НШ в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i=d_iG(\mathrm{mod}q)$	(d_i, Q_i)	$a, b, G, n, f(x)(P), h$	Q_i	Експоненційна
НШ в гіпереліптичних кривих	C_i	$D_2= c_iD_1$	(c_i, D_2)	$f(x), g(x), q, D_1, g, J$	D_2	Експоненційна
НШ зі спарюванням точок еліптичних кривих	$d_{iD}=s\ Q_{iD}$	$Q_{iD}=H_1(ID)$	(d_{iD}, Q_{iD})	$G_1, G_2, e, H_1, P, H_2, H_3, F_2{}^m, P_p$	Q_{iD}	Експоненційна – субекспоненційна
НШ в кільці зрізаних поліномів (NTRU)	$f = 1+pF(\mathrm{mod}q)$	$h=f^{-1}*g*p(\mathrm{mod}q)$	(f,h)	N, q, p, f, g, df, dg, c		Експоненційна – субекспоненційна

Як випливає з таблиці 2, в якості (сертифіката) відкритого ключа направленого шифрування в RSA системі використовується відкритий Еі ключ із* асиметричної пари ключа (Di, Ei), а в якості особистого (таємного) ключ Di. Для асиметричного криптографічного перетворення в полі Галуа як (сертифікат) відкритого ключа направленого шифрування використовується елемент поля Yi, а як особистий ключ – ціле число Xi.Для асиметричного криптографічного перетворення в групі точок еліптичних кривих як сертифікат відкритого ключа направленого шифрування використовується точка еліптичної кривої Qi, а як особистий ключ електронного цифрового підпису – ціле число di. При застосуванні криптографічного перетворення на гіпереліптичних кривих як сертифікат відкритого ключа використовується якобіан D2, а як особистий ключ – *якобіан D1*. При застосуванні криптографічного перетворення зі спарюванням точок еліптичних кривих як сертифікат відкритого ключа направленого шифрування використовується ключ Q_{iD}, а як особистий ключ – d_{iD}. *Особливий інтерес нині мають ІВК, що ґрунтуються на криптографічних перетвореннях в кільці урізаних поліномів[6 -7].* Основною перевагою цього алгоритму є те, що він працює набагато швидше звичайних алгоритмів направленого шифрування з відкритим ключем, наприклад таких як RSA. Перевага у швидкості є особ-

ливо великою в генерації ключів, яке найчастіше є найбільш важливою частиною у криптографії з відкритим ключем. Для ЕЦП пряме перетворення виконується на особистому ключі, а зворотне на відкритому.

2. Стан створення та застосування ІВК для виготовлення та використання машиночитаємих документів.

В процесі інтеграції України на міжнародному рівні взагалі та в Європейський Союз для України дуже актуальними є задачі створення та розвитку національної системи біометричної верифікації і ідентифікації громадян, а також в цілому систем виготовлення та обігу ICAO – сумісних на міжнародному рівні електронних документів, включаючи електронні біометричні паспорти[8,11,12]. Безумовно важливою та необхідною цієї системи є інфраструктура відкритих ключів (ІВК). Україна в короткий час під загальним керівництвом EDAPS створила та практично ввела в експлуатацію вказану систему, що повністю сумісна на міжнародному рівні. Функціональна схема ІВК системи наведена на рис. 1. В процесі досліджень для ІВК, що наведена на рис. 1,визначено перелік основних загроз , до яких відносяться такі: компрометація змісту об'єкту захисту документу і логічної структури даних; точне копіювання або підміна чипу; скіммінг (зчитування без прямого доступу до паспорта); несанкціонований доступ до чипу паспорту та перехоплення інформації при обміні з терміналом.

Захист від вказаної множини загроз забезпечується засобом застосування таких механізмів захисту: пасивна автентифікація – для захисту від компрометації змісту об'єкту захисту документу і логічної структури даних; активна автентифікація – для захисту від точного копіювання або підміни чипу; розширений контроль даних – для захисту від несанкціонованого доступу; шифрування даних – для захисту додаткових біометричних параметрів.

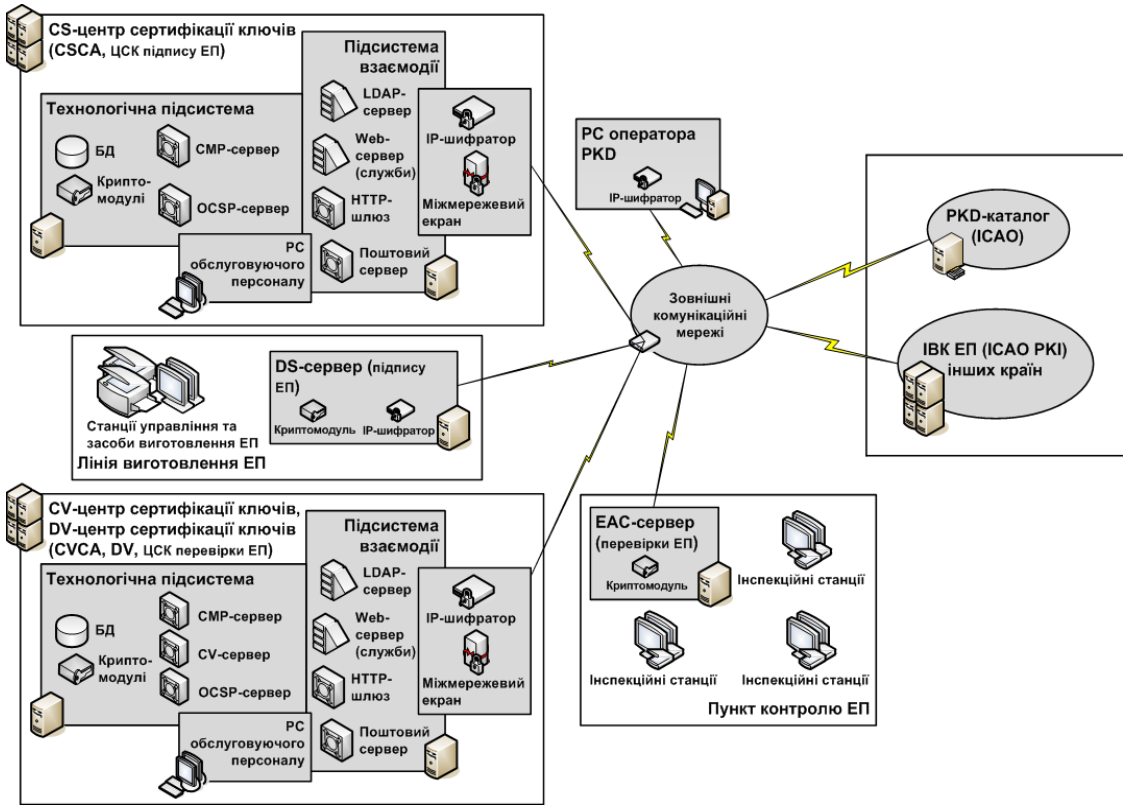

Рис. 1 - Функціональна схема ІВК для біометричного паспорту

Такий вибір не суперечить рекомендаціям та стандартам - ICAO рекомендує застосовувати два механізми перевірки біометричного електронного паспорту – пасивну та активну автентифікацію. Пасивна автентифікація є обов'язковою і призначена для автентифікації даних, які зчитані з електронного паспорту. Вона здійснюється шляхом перевірки підпису на зчитаних даних, використовуючи відповідний сертифікат ЦСК країни, що випустила паспорт. Активна автентифікація є необов'язковою і може використовуватися для перевірки чипу на справжність (автентичність).

Базовий контроль доступу є механізмом автентифікації та призначений для запобігання скіммінгу та перехоплення передачі повідомлень між машино зчитувальним проїзним документом і системою перевірки IS, його застосування є обов'язковою умовою для впровадження розширеного контролю доступу – механізму, що забезпечує захист від несанкціонованого доступу до додаткових біометричних даних.

Безпосередньо ІВК України створюється, як складова частина системи виготовлення та обігу біометричних паспортів у відповідності до технічних вимог ICAO. Її основою є програмно – технічний комплекс. Комплекс та його складові частини повинні відповідати технічним вимогам ICAO та правилам посиленої сертифікації. Він також повинен забезпечити реалізацію регламентних процедур та механізмів функціонування ІВК відносно обслуговування сертифікатів відкритих ключів; надання засобів КЗІ для використання у складових частинах інфраструктури під час виготовлення та перевірки біометричних

Функціональна схема діючого програмно – технічного комплексу наведена на рис. 1. Основними елементами комплексу є: CS-центр сертифікації ключів (CSCA, ЦСК підпису електронних паспортів); CV-центр сертифікації ключів (CVCA, ЦСК перевірки біометричних паспортів) , що суміщений з DV-центром сертифікації ключів (DV, що є версифікатором електронного паспорту; робоча станція (PC) оператора PKD (CIL); DS-сервер (сервер підпису електронних паспортів);EAC-сервер (сервер перевірки біометричних паспортів).

На основі аналізу в процесі розробки визначені вимоги до структури та призначення комплексу технічних засобів CS-ЦСК, вимоги до характеристик комплексу, що наведені у таблиці , вимоги до режимів функціонування комплексу, вимоги до режимів функціонування комплексу та до експлуатації комплексу.

Основні характеристики програмно - технічного комплексу наведені в таблиці 3.

Таблиця 3 – Основні характеристики комплексу.

Показник	Значення
Число одночасних підключень до серверів взаємодії CS-ЦСК та CV/DV-ЦСК – LDAP-каталогу та web-сторінки	не менше 1 000
Час обробки ЦСК запитів на формування, блокування, поновлення та скасування сертифікатів	не більше 1 с (не менше 20 запитів/с)
Час обробки ЦСК запитів на визначення статусу сертифіката	не більше 1 с (не менше 100 запитів/с)
Час формування ЕЦП при підписі даних паспорту	не більше 0.05 с (не менше 20 запитів/с)
Кількість одночасних підключень до серверів взаємодії CS-ЦСК та CV/DV-ЦСК – LDAP-каталогу та web-сторінки)	не менше 1 000
Час обробки ЦСК запитів на формування, блокування, поновлення та скасування сертифікатів	не більше 1 с (не менше 20 запитів/с)
Час обробки ЦСК запитів на визначення статусу сертифіката	не більше 1 с (не менше 100 запитів/с)
Час формування ЕЦП при підписі даних паспорту	не більше 0.05 с (не менше 20 запитів/с)

Для визначення степеню виконання ти функціональних вимог були використані у відповідності до стандарту ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation) [9,10] критерії оцінки електронних проїзних документів. Застосування стандарту ISO/IEC 15408 дозволяє забезпечити умови, в яких процес опису, розробки та перевірки продукту буде проведений з виконанням необхідних вимог. Функціональні вимоги безпеки для біометричних паспортів наведені в таблиці 4.

Таблиця 4 - Функціональні вимоги безпеки для електронних паспортів.

Функціональний клас безпеки	Функціональна складова безпеки
Криптографічна підтримка (FCS)	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1
Конфіденційність (FPR)	FPR_UNO.1
Захист даних користувача (FDP)	FDP_ACC.1, FDP_ACF.1, FDP_RIP.1, FDP_UCT.1, FDP_UIT.1
Ідентифікація та автентифікація (FIA)	FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.1
Менеджмент безпеки (FMT)	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.3, FMT_SMF.1, FMT_SMR.1
Захист TSF (FPT)	FPT_FLS.1, FPT_ITI.1, FPT_RVM.1, FPT_SEP.1, FPT_TST.1

Таким чином в цілому функціональні вимоги до електронного біометричного паспорту, в найбільш прийнятній формі можна задати при використанні стандарту ISO/IEC 15408.

3. Сутність та застосування ІВК в АБС банків.

ІВК є також основою для надання усіх вказаних вище послуг в банківських системах, перше за все в системах Клієнт – Сервер. Спосіб використання засобів реалізації ІВК для таких систем наведено на рис. 2. Функціональна схема ЦСК наведена на рис.3. Важливими є також питання, що пов’язані з використанням криптографічних систем та механізмів, а також криптографічних протоколів та технічних специфікацій. Вказані дані наводяться нижче.

Рис. 2 - Використання засобів КЗІ

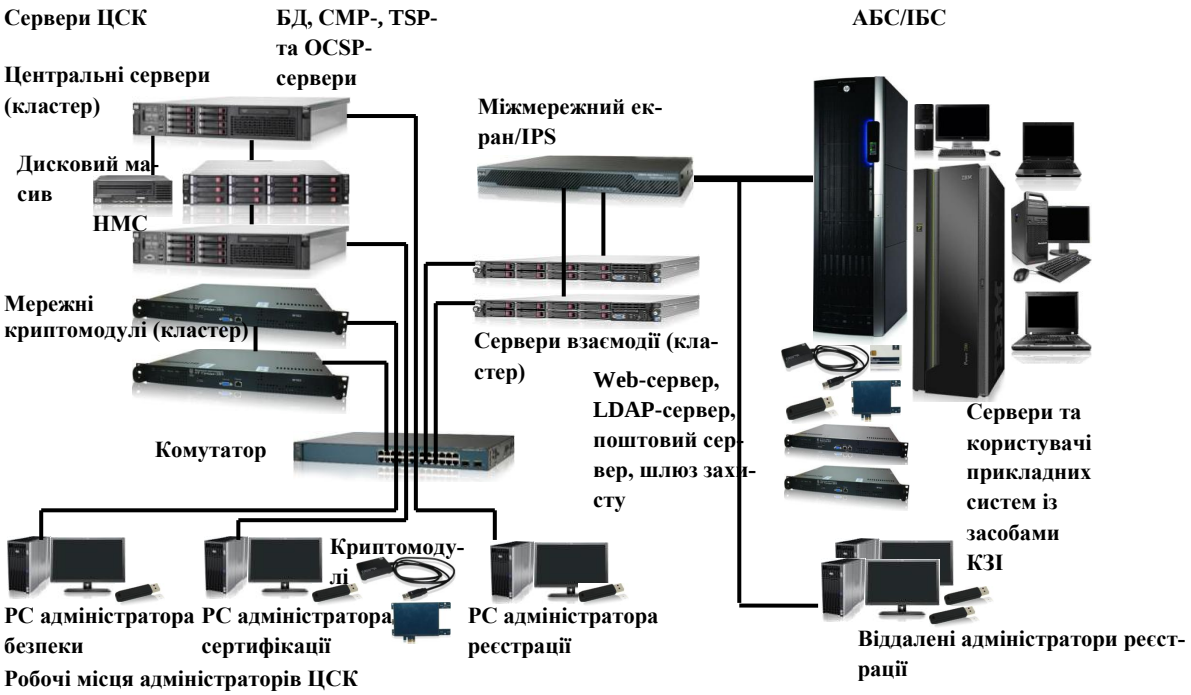

Рис. 3 - Функціональна схема ЦСК банку

Основними елементами центру сертифікації ключів є такі:

– Програмний комплекс ЦСК “ІІТ ЦСК-2” (програмні комплекси центрального сервера взаємодії, адміністраторів ЦСК та віддаленого адміністратора реєстрації).

– Програмний комплекс користувача ЦСК “ІІТ Користувач ЦСК-2” (засоби електронного цифрового підпису, шифрування та автентифікації, у т.ч. бібліотека користувача ЦСК).

– Апаратні криптомодулі “Гряда-52” та “Гряда-61”.
– Мережний криптомодуль “Гряда-301”.
– Електронний ключ “Кристал-1”.
– Старт-карта “Гряда-301”.

Криптографічні алгоритми та протоколи:
– Шифрування за ДСТУ ГОСТ 28147:2009.
– Електронний цифровий підпис (ЕЦП) за ДСТУ 4145-2002.
– Гешування за ГОСТ 34.311-95.
– Протокол розподілу ключових даних за ДСТУ ISO/IEC 15946-3 та державних технічних специфікацій.
– Протокол взаємної автентифікації за ДСТУ ISO/IEC 9798-3.
– Шифрування TDEA та AES за ISO/IEC 18033-3.
– ЕЦП RSA за ISO/IEC 14888-2:2008 та PKCS#1, DSA за ISO/IEC 14888-3 та ECDSA за ISO/IEC 15946-2.
– Протоколи розподілу ключових даних DH за ISO/IEC 11770-3:2008 та ECDH за ISO/IEC 15946-3.
– Гешування SHA за ISO/IEC 10118-3:2004.

Формати даних та протоколи взаємодії:
– Сертифікати та списки відкликаних сертифікатів (СВС) згідно ISO/IEC 9594-8 та державних технічних специфікацій.
– Протокол OCSP (визначення статусу сертифіката) згідно RFC 2560 та державних технічних специфікацій.
– Протокол TSP (фіксування часу) згідно RFC 3161 та державних технічних специфікацій.
– Підписані дані (дані з ЕЦП) згідно ETSI TS 101 733 (CAdES), RFC 5652 та державних технічних специфікацій.
– Захищені дані (зашифровані дані) згідно RFC 5652 та державних технічних специфікацій.
– Особисті ключі згідно PKCS#8 та PKCS#12.

Засоби захисту АБС на платформі SAP for banking.
Забезпечують у складі АБС:
– цілісність та неспростовність авторства електронних даних та документів, що циркулюють у системі;
– автентифікацію користувачів АБС та конфіденційність і цілісність даних, які передаються між користувачами та сервером системи.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у АБС, реалізуються шляхом формування та перевіряння ЕЦП від даних та документів, як на стороні користувача АБС (SAP-клієнта) так і на стороні сервера (SAP-сервера).

Аутентифікація користувачів АБС (SAP-клієнтів) на сервері (SAP-сервері) здійснюється під час підключення користувачів до сервера (встановлення з’єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером АБС під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Засоби захисту ІБС на платформі Oracle Flexcube.
Забезпечують у складі ІБС:

– цілісність та неспростовність авторства електронних даних та документів, що циркулюють у системі;

– автентифікацію користувачів ІБС та конфіденційність і цілісність даних, які передаються між користувачами та сервером системи.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у ІБС, реалізуються шляхом формування та перевіряння ЕЦП від даних та документів, як на стороні користувача ІБС (FlexCube-клієнта - web-оглядача) так і на стороні сервера (FlexCube-сервера).

Автентифікація користувачів ІБС (FlexCube-клієнтів - web-оглядачів) на сервері (FlexCube-сервері) здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером через шлюз захисту) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером ІБС (шлюзом захисту) під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум даних TCP-з'єднання.

4. Основні напрями розвитку та удосконалення ІВК.
Перспективна система шифрування на основі NTRU.

В середині 1990-х років групою математиків (ДжефріХовстейн, ДжиллПіфер та Джозеф Сильверман) було розроблено новий алгоритм який отримав назву NTRU[6,7]. В 1998 році було опубліковано повний опис алгоритму та його аналіз Основною перевагою цього алгоритму є те, що він працює набагато швидше звичайних алгоритмів з відкритим ключем, таких як RSA. Перевага у швидкості є особливо великою в генерації ключів, яке найчастіше є найбільш важливою частиною у криптографії з відкритим ключем. Розглянемо ідеї, що лежать в основі NTRU для застосування при направленому шифруванні та цифровому підписі.

У алгоритмі NTRU усі операції здійснюються в кільці усічених многочленів. Криптографічна стійкість алгоритму заснована на складності вирішення задачі знаходження короткого вектора у заданій решітці. NTRU працює, як вже згадувалось, швидше ніж криптосистеми з відкритим ключем, які застосовуються зараз. Для за шифрування та розшифрування повідомлення довжиною з N символів необхідно $O(N^2)$ операцій для крипто системи, в той час як для RSA потрібно $O(N^3)$ операцій. В таблиці 5 наведені основні параметри NTRU

Таблиця 5 - Параметри основного алгоритму

Параметр	Коротке пояснення параметру
N	Розмір усіченого кільця многочленів R. Елементи кільця представлені у вигляді поліномів ступеня N – 1(не секретний)
q	Великий модуль по якому приводиться кожний коефіцієнт многочлена у кільці R (не секретний)
p	Малий модуль по якому приводиться кожний многочлен (не секретний)
f	Многочлен, який є секретним ключем
g	Многочлен, який використовується для генерації публічного ключа h з f (секретний але відкидається після першого використання)
h	Публічний ключ, теж многочлен
r	Випадковий «забілюючий» многочлен (секретний але відкидається після першого використання)
df	f має df коефіцієнти еквівалентні 1 та df-1 коефіцієнти еквівалентні - 1
dg	g має dg коефіцієнти еквівалентні 1 та dg коефіцієнти еквівалентні - 1
dr	r має dr коефіцієнти еквівалентні 1 та dr коефіцієнти еквівалентні - 1

Основною перевагою, в тому числі і відносно криптосистем на еліптичних кривих, є можливість підвищення швидкодії на 2 – 3 порядки.

Основні проблемні питання розвитку системи ЕЦП України

В якості першочергових потрібно вирішити такі завдання:

- створення та застосування у існуючих та перспективних системах ІВК, сумісних з Європейськими та міжнародними;
- забезпеченням необхідних рівнів гарантій надання послуг з безпеки інформації;
- використанням досвіду технологічно розвинених держав, Європейської та міжнародної стандартизації, уніфікації тощо;
- поставка замовникам уніфікованих елементів ІВК та центрів сертифікації різного призначення та можливостей;
- надання користувачам послуг ІВК з вищим (апаратним) та середньо апаратним рівнями гарантій згідно ISO/IEC 15408;
- уніфікація та стандартизації національної ІВК, включаючи національну систему ЕЦП;
- удосконалення методів та алгоритмів криптографічних перетворень по критерію мінімізації складності операцій;
- розвиток математичних методів та систем крипто аналізу, прогнозування вимог і умов та обмежень відносно застосування стандартизованих криптографічних примітивів та криптографічних протоколів, їх удосконалення;
- дослідження та прогнозування розвитку та удосконалення міжнародних ІВК, врахування їх досвіду та результатів, гармонізація національної системи ЕЦП з міжнародними ІВК та ІВК технологічно розвинених держав.

При урахуванні вказаних пропозицій появиться можливість:

- вирішити низку наукових та практичних задач розвитку теорії та практики побудування ІВК, в тому числі система ЕЦП України як для внутрішньо державного так і міжнародного застосувань;
- отримати методики та засоби обґрунтування вимог, експериментального та практичного дослідження алгоритмів та засобів ЕЦП та порівняння існуючих стандартів ЕЦП;
- розробити методи та системи оцінки стійкості криптографічних перетворень в групах точок еліптичних та гіпереліптичних кривих, а також зі спарюванням точок еліптичних кривих;
- впровадити технічні специфікації відносно форматів даних та протоколів взаємодії в системі ЕЦП у відповідності з міжнародними вимогами;
- розробити апаратні засоби КЗІ, які будуть забезпечувати вищий рівень гарантій та можливість відображення політики на міжнародному та міждержавному рівнях;
- економічно обґрунтована ІВК, включаючи декілька засвідчувальних центрів та сукупності АЦСК та ЦСК , а також узгоджене впровадження системи відокремлених пунктів, включно до районних адміністративних одиниць;
- розробити та впровадити науково - обґрунтовану систему підготовки та перепідготовки спеціалістів, що задіяні в обслуговуванні, розробці, проведенні експертизи та експлуатації системи ІВК (ЕЦП);

Впровадження вказаних пропозицій дозволить створити в Україні конкурентоспроможні елементи і безпосередньо систему ІВК для усіх існуючих застосувань, яка за своїми характеристиками, в першу чергу рівнем гарантій надання послуг та криптографічної стійкості криптографічних примітивів, що будуть застосовуватись, що будуть відповідати міжнародним вимогам.

Література:

1.Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.

2.Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
3.Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.
4.ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8:2006»Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів. ».
5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010, 593с.
6. Joseph H. Silverman, Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem, NTRU Cryptosystems Technical Report 13, available at http://www.ntru.com.
7. J. H. Silverman and W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt. Technical Report #18
8. ICAO9303-pt1-vol2.
9. ISO/IEC 15408: 2000 – Information technology – Security techniques – Evaluation criteria for IT security. Part 1-3.
10. FIPS-186-3 - Information Technology Laboratory - National Institute of Standards and Technology - Digital Signature Standard (DSS), 2006.
11. Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents - Exended Access Control (EAC),Password Authenticated Connection Establishment (PACE)and Restricted Identification (RI), Version 2.05, TR-03110, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2010. 9
12. ePassport Protection Profile V1.0, National Intelligence ServiceIT Security Certification Center