УДК 004.056:[336.71(430)+336.71(477)]

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ НАЦІОНАЛЬНИХ БАНКІВ УКРАЇНИ ТА НІМЕЧЧИНИ

Ю.І. ГОРБЕНКО, І.Ф. АУЛОВ, Є.Ю. КУТЯ, Д.Е. ХРЯПІН

Наводяться результати аналізу та порівняння криптографічних примітивів, що застосовуються та плануються до застосування для захисту інформації в банківських інформаційних технологіях України та Німеччини. Визначено перелік стандартів, що пропонується до впровадження та застосування на території України

Ключові слова: криптографічні системи, криптографічні примітиви.

ВВЕДЕННЯ

Нині в Україні створені та надійно функціонують банківські інформаційні технології та системи. По суті, починаючи з 1992 року в них значна увага приділяється питанням захисту банківської інформації [проект CrypTool, 1], створені та функціонують комплексні системи захисту інформації. Обов'язковими послугами, що повинні надаватись в них клієнтам та власникам, є такі послуги, як неспростовність, цілісність, справжність, доступність, конфіденційність та надійність [ISO 15408]. Якість надання вказаних послуг та рівень гарантій в суттєвій мірі визначається методами (перетвореннями), механізмами та протоколами криптографічного захисту інформації. Також визнано, що для надання вказаних послуг з необхідним рівнем гарантій необхідно використовувати асиметричні та симетричні криптографічні перетворення, а також криптографічні протоколи автентифікації та встановлення ключів, що на них ґрунтуються.

Одним із проблемних питань надійного функціонування банківських інформаційних технологій є забезпечення інтероперабельності, в тому числі в частині криптографічного захисту інформації. Зважаючи на актуальність вказаних задач, в Україні та Германії широко застосовуються міжнародні та національні стандарти, а також рекомендації, що визначають вимоги до систем обробки та захисту інформації [проект CrypTool,1]. Проте, як показав аналіз, в обох державах виникають проблемні питання забезпечення інтероперабельності, як у плинний час, так і з прийняттям нових та оновленням стандартів та рекомендацій, що є необхідним при взаємодії на міжнародному та міждержавному рівнях. Тому, на наш погляд, важливою є задача вивчення та порівняння стану застосування криптографічних перетворень та механізмів, перше за все в частині стандартизації.

Результати попереднього аналізу показали, що в Німеччині зроблені суттєві кроки та отримані певні результати в частині використання методів та протоколів криптографічного захисту інформації [2]. У зв'язку з цим для України важливим є вивчення досвіду Німеччини та визначення можливостей його застосування в частині криптографічного захисту інформації взагалі та у банківській сфері частково.

Що стосується стандартизації, то потрібно відмітити, що значна частина європейських та міжнародних стандартів захисту інформації була досліджена та/або запропонована інститутами Німеччини [Sigen, Duisburg (Prof. Weis), Darmstadt (Prof. Eckert)]. Вказане дозволяє зробити висновок про досить високий рівень забезпечення безпеки інформації у Німеччині. Державною структурою Німеччини, що впроваджує загальнодержавну політику безпеки, є Федеральне Бюро Інформаційної Безпеки (BSI) [2]. Цією структурою було розроблено ряд систем здійснення захищених транзакцій банками. До них відносяться: Захищені електронні транзакції (SET), Електронна готівка (ecash), Кібер Монета (CyberCoin), Мілі-цент (Millicent) та Комп'ютерний Інтерфейс Домашнього Банкінгу (HBCI) [3]. Для реалізації захисту інтернет-банкінгу, тобто для захисту взаємодії між клієнтом та банком, використовують звичайну Інтернет мережу. Часто застосовується протокол Secure Socket Layer (SSL), а також при реалізації цифрового підпису та направленого шифрування криптоперетворення на основі асиметричного криптографічного алгоритму RSA, але уже з ключами довжиною не менше, ніж 2048 біт [4].В якості симетричних крипто перетворень застосовуються симетричні алгоритми шифрування triple-DES та IDEA, а у якості функції гешування RIPEMD-160 [4].

В цілому, Німеччина в частині застосування криптографічних примітивів та протоколів в першу чергу орієнтується на систему стандартизації США та ЄС.

Метою цієї статті є оцінка та порівняльний аналіз якості криптографічного захисту платіжної інформації в банківській сфері Німеччини та України та інтероперабельності в частині захисту інформації на внутрішньому та міжнародному рівнях.

В подальшому під криптографічними системами ми будемо розуміти все, що стосується криптографічних примітивів та протоколів.

1. КРИТЕРІЇ ТА ПОКАЗНИКИ ПОРІВНЯННЯ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Першим, що є необхідним для оцінки та порівняння криптографічних систем, є вибір критеріїв та показників оцінки криптографічних сис-

тем. Основними стандартами, які розглядаються та аналізуються в цій статті, є стандарти різних рівнів, що застосовуються у Німеччині. В першу чергу це стандарти FIPS 186-3; ISO/IEC 14888-1,2,3; ISO/IEC 18033-1,2,3,4 та FIPS 180-3 [2]. Відносно України, то це стандарти ДСТУ ГОСТ 34.311-2009; ДСТУ ГОСТ 28147-2009, ДСТУ 4145-2002 [5, 6, 7], а також FIPS 186-3 ISO/IEC 14888-1,2,3; ISO/IEC 18033-1,2,3,4 та FIPS 180-3 [8, 9]. Також в якості перспективних розробок будемо розглядати симетричні криптографічні примітиви – блокові симетричні шифри, що розглядались на національному конкурсі в Україні[10].

В подальшому, зважаючи на те, що симетричні та асиметричні криптографічні примітиви та функції гешування мають свої особливості, при їх порівнянні будемо використовувати критерії та показники, які дозволяють врахувати їх специфіку. Так для оцінки криптографічних примітивів запропоновані критерії та показники, за якими здійснюється порівняльний аналіз. Також у відповідності до [11] будемо задавати і основні вимоги блочних симетричних шифрів. Наявність вимог дозволяє застосувати при порівнянні і відповідні критерії.

Для блочних та поточних симетричних шифрів в якості критеріїв та показників порівняння вибрані:

– показник – бітова довжина ключових даних;

– критерій – наявність слабких ключів;

– критерій – стійкість схеми розгортання ключів;

– критерій – стійкість проти атаки груба сила та аналітичних атак.

В якості вимог до блочних симетричних шифрів, висунуті такі:

– повинен розроблятися відкрито та обиратися на міжнародному рівні (бути міжнародним стандартом);

– повинен працювати з блоками та ключами довжиною 128, 256, 512 бітів;

– повинен функціонувати в п'яти основних режимах роботи, що визначені стандартами;

– не мати слабких ключів;

– мати стійку схему розгортання ключів;

– генерування ключів у відповідності до визнаних стандартів.

Для асиметричних крипто перетворень були обрані наступні показники та критерії порівняння:

– показник – бітова довжина ключових даних та вимоги до модуля перетворення;

– критерії – наявності та сутності таємних та відкритих параметрів шифру;

– критерій – стійкість проти «атак на зв'язаних ключах» та атак типу «Повне розкриття»;

– критерій – складність вироблення та перевірки ЕЦП.

В якості вимог до асиметричних перетворень висунуті такі:

– використання модуля перетворення в кільці та полі довжиною не менше, ніж 2048 бітів;

– використання модуля перетворення в групі точок еліптичної кривої довжиною не менше, ніж 192 біта;

– генерування ключів та загальних параметрів у відповідності до визнаних стандартів.

Функції гешування порівнюються за наступними показниками та критеріями:

– показник – розмір блоку повідомлення, що обробляється;

– показник – розмір геш-значення, в яке відображається повідомлення;

– показник – число раундів перетворення;

– показник – максимальна довжина повідомлення, для якої може бути обчислене геш-значення.

В якості загальних вимог до криптографічних примітивів можна висунути наступні:

– алгоритм повинен бути орієнтованим для можливості реалізації на 32-х або 64-х розрядних процесорах;

– зазначені в алгоритмі операції повинні мати по можливості більш ефективну програмну та/або апаратну (апаратно-програмну) реалізацію;

– необхідний для роботи об'єм пам'яті має враховувати можливість реалізації алгоритму у мікро пристроях;

– передбачити можливість паралельного виконання декількох операцій.

Також підкреслимо під критерієм ми будемо розуміти ознаку, на основі якої здійснюється класифікація, оцінка, порівняння, тобто мірило оцінки.

2. РЕЗУЛЬТАТИ ПОРІВНЯННЯ СИМЕТРИЧНИХ КРИПТОСИСТЕМ

Зважаючи на великі обсяги інформації, що обробляються в банківських інформаційних технологіях, як правило, для забезпечення послуг цілісності, справжності та конфіденційності, доцільно застосовувати симетричні криптографічні перетворення.

В табл. 1 та 2 наведені результати порівняння симетричних криптографічних систем: потокових та блокових симетричних шифрів, що застосовуються або можуть застосовуватись в Україні та Німеччині.

З результатів порівняння видно, що в Німеччині діє велика кількість міжнародних стандартів, що надає можливості застосування різних криптографічних систем. В Україні в якості блокового або потокового шифру може використовуватися лише ГОСТ-28147-89 в різних режимах його роботи, при цьому ГОСТ-28147-89 забезпечує тільки задовільний рівень стійкості. Для забезпечення високого та надвисокого рівнів стійкості необхідно застосовувати для внутрішніх систем блоковий симетричний шифр Калина, а на міжнародному AES та SNOW-2. В цьому випадку буде забезпечено не тільки високі рівні стійкості, а і стандартизація та уніфікація і на міжнародному рівні.

Таблиця 1

Порівняння параметрів симетричних криптографічних систем

	Германія			Україна		
Шифр	SNOW-2	TDES	AES	Мухомор	ГОСТ28147-89	Калина
Параметри	Т: Вектор ініціалізації IV, ключ К	Т: Ключі k_1, k_2, k_3	В: Число циклів Т: Ключ К	В: Число циклів Т: Ключ К	В: Число раундів Т: ключ K_c,$K_д$.	В: Число циклів Т: Ключ К
Довжина ключа, біт	К=128, 256 IV=128	168 (3 ключі по 56)	128,192, 256	128-512	K_c= 256 $K_д$ = 512	128, 256, 512

Таблиця 2

Порівняння стійкості симетричних криптографічних систем

	Германія			Україна		
Шифр	SNOW-2	TDES	AES	Мухомор	ГОСТ-28147	Калина
Наявність слабких ключів	Ні	Так	Ні	Ні	Так	Ні
Аналітичні атаки	Ні	2^{113}	Ні	Ні	Так	Ні
Груба сила	2^{256}	2^{168}	$2^{128} – 2^{256}$	2^{512}	2^{64}	2^{512}
Розгортання ключів	Ні	Слабка	Слабка	Ні	Слабка	Ні

3. РЕЗУЛЬТАТИ ПОРІВНЯННЯ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Порівняння асиметричних криптосистем зробимо на прикладі «електронних грошей». Сьогодні вони вирішують більшість проблем готівкових грошей. Основними з них є такі як потреба в місці для збереження, складність перевезень, підрахунку, розрахунків за допомогою готівки, конвертація валют, невеликий строк їх служби тощо. Але в той же час при їх використанні постають нові задачі, які потребують вирішення. До них необхідно віднести такі:

– операції банка та клієнта (наприклад домашній банкінг, телефонний банкінг), які використовуються для того, щоб управляти рахунком клієнта;

– угоди клієнт-продавець. Вид операцій, при яких продавець надає клієнту якусь послугу та отримує від нього електронні гроші. До цих операцій відносяться такі, що виконуються за використанням телекомунікаційних систем, наприклад відвідуванням інтернет магазинів;

– угоди клієнт – посередник – продавець. Це тип угод, при яких оплата виконується з використанням якоїсь третьої сторони. Це може бути банк, або кредитна компанія, або інша структура, що є посередником між клієнтом та продавцем.

Аналіз показав, що для Європейських центральних банків особливо важливим є те, щоб громадськість мала довіру до новітніх систем оплати та «електронних грошей». Тому клієнтам має надаватися захист від шахрайства та підробки, в тому числі і шахрайства зі сторони самого банку. Тому в таких системах повинно надаватись також послуги неспростовності об'єктів та суб'єктів взаємодії. Вказане може досягатись на основі використання асиметричних криптографічних перетворень [8]. Крім того, при реалізації криптографічних механізмів та протоколів автентифікації, встановлення, узгодження, передавання та транспортування ключів, розподілу таємниці, тощо, виникає необхідність використання як симетричних, так і асиметричних, так і симетричних крипто перетворень.

В таблиці 3 наведені результати порівняння асиметричних криптографічних систем – міжнародних та регіональних стандартів.

Проаналізуємо в першу чергу відмінності алгоритмів. Так в алгоритмах EC-DSA, EC-GDSA, EC-KCDSA використовується поле GF(p), а в стандарті України ДСТУ 4145-2002 $GF(2^m)$. В алгоритмі EC-KCDSA, на відміну від алгоритмів EC-DSA та EC-GDSA, для перетворення точки еліптичної кривої в ціле число використовується функція гешування.

Таблиця 3

Порівняння параметрів асиметричних криптографічних систем

		EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	RSA	DSA (FIPS-186-3)
Параметри		B:a, b, G, n, f(x), m, U, h, Q				B: D	B: x
		T: d	T: d^{-1}	T: d^{-1}	T: -d	T: E, p, q,ϕ(N)	T: P, q, a
Вимоги до n та d		$n \geq 2^{192}$ $1<d<n-1$			$2^{163} \leq n \leq 2^{509}$ $1<d<n-1$	$n \geq 2^{2048}$ $1<d<n-1$	$2^{511} \leq P \leq 2^{1024}$ $1<x< q-1$
Стійкість проти атак	на зв'язаних ключах	Ні	Неповністю	Так	Ні	Неповністю	
	повне розкриття	$k\sqrt{n}$				$e^{\delta (\ln N)^{\nu} (\ln\ln N)^{1-\nu}}$	

При виробленні електронного цифрового підпису та при його перевірянні в алгоритмах EC-KCDSA та EC-GDSA не виконуються обчислення мультиплікативної інверсії за модулем, що дозволяє зменшити складність вироблення підпису. В свою чергу використання в якості особистого ключа –d в алгоритмі ДСТУ 4145-2002 також дозволяє не обчислювати мультиплікативну інверсію за модулем. В цілому результати аналізу дозволили зробити висновок, що національний стандарт ДСТУ 4145-2002 відповідає міжнародно-визнаним вимогам і може бути застосований для направленого шифрування та встановлення ключів. На відміну від України, Німеччина використовує у якості алгоритми ЕЦП, ще і RSA та DSA, що представлені в FIPS 186 – 3[12].

Результати порівняння складності електронних цифрових підписів наведені в табл. 4.

4. РЕЗУЛЬТАТИ ПОРІВНЯННЯ ФУНКЦІЙ ГЕШУВАННЯ

Для вирішення задач забезпечення цілісності та справжності інформації застосовуються криптографічні контрольні суми[5,13]. Методи формування криптографічних контрольних сум можна розділити на два великі класи: на базі симетричних криптографічних перетворень і на базі асиметричних перетворень,. Такі функції можуть застосовуватися як безпосередньо, так і в інших перетвореннях, це таких, як електронний цифровий підпис, де необхідна ефективна функція відображення повідомлення в образ невеликої фіксованої довжини. Порівняння функцій гешування за запропонованими критеріями наведено в табл. 5.

Необхідно відмітити, що стосовно функцій гешування Німеччина пішла проти світових тенденцій та відмовилась від використання геш – функції SHA-1, що видно з таблиці 5. Замість неї Німеччина стала використовувати функцію гешування RIPEMD-160.

Згідно офіційних публікацій BSI функцію SHA-1 можна використовувати до 2009 року лише для алгоритмів, що пов'язані з підписанням сертифікатів відкритих ключів. До 2010 року SHA-1 може використовуватися лише в алгоритмах підпису сертифікатів відкритих ключів, але тих, що мають не менше 20 бітів ентропії в серійному номері. В подальшому функції гешування RIPEMD-160 та SHA-1 можуть бути застосовані лише для перевірки сертифікатів відкритих ключів. Замість цих функцій, в банках Німеччини будуть застосовуватися сімейство функцій SHA-2 з різними довжинами геш повідомлень.

Також національний інститут стандартизації США (NIST) в результаті появи ряду атак з використанням методу створення колізій на функцію гешування SHA-1, вже в 2007 році розпочав відкритий конкурс на проект нового стандарту гешування, який отримав назву SHA-3.

Що стосується України, то міждержавний стандарт ГОСТ 34.311-95 також припинить свою чинність в 2010 році, тому в Україні доцільно провести роботи з прийняття нового стандарту, а також з впровадження міжнародного стандарту ISO/IEC 10118-3.

5. СТАН ВПРОВАДЖЕННЯ МІЖНАРОДНИХ ТА РЕГІОНАЛЬНИХ СТАНДАРТІВ

Проведений аналіз показав, що Німеччина суттєву увагу приділяє питанням міжнародної та регіональної стандартизації, а також забезпеченню інтероперабельності криптосистем та криптопротоколів. По суті, в реальних системах застосовуються європейські, міжнародні та федеральні стандарти США. Україна також веде деяку роботу в цьому напрямі, але з прийняттям та введенням в дію стандартів велика затримка. В табл. 6 наведені результати порівняльного аналізу стану застосування криптографічних протоколів. Їх результати дозволяють зробити висновок, що Україна суттєво відстає в планів провадження крипто протоколів та їх гармонізації з Європейськими та міжнародними.

Таблиця 4

Складність алгоритмів ЕЦП України і Німеччини

	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ 34.310-2001
Складність вир. ЕЦП	1h+1π+1div+ 2mul+1add+1s	1h+1π+0div+ 2mul+1add+1s	2h+0π+0div+ 1mul+1add+1s	1h+1π+0div+ 2mul+1add+1s	1h+1π+1div+ 2mul+1add+1s
Складність пер. ЕЦП	1h+1π+1div+ 2mul+2s+1sad	1h+1π+1div+ 2mul+2s+1sad	2h+0π+0div+ 0mul+2s+1sad	1h+0π+0div+ 1mul+2s+1sad	1h+1π+1div+ 2mul+2s+1sad

Таблиця 5

Порівняння геш-функцій

Назва геш-функції	SHA-1	SHA 2				RIPEMD-160	ГОСТ 34.311-95
		224	256	384	512		
Рік до якого дійсна	2009	2015	2016	2016	2016	2010	2010
Розмір блоку	512	512	512	1024	1024	512	256
Розмір повідомлення геш	160	224	256	384	512	160	256
Число раундів	80	64	64	80	80	5	1
Максимальна довжина повідомлення	2^{64}-1	2^{64}-1	2^{64}-1	2^{128}-1	2^{128}-1	2^{64}-1	2^{105}

Таблиця 6

Порівняльний аналіз криптографічних систем національних банків України та Німеччини

Критерій	Німеччина	Україна
1) Крипто-примітиви, що використо-вуються в протоколах	– симетричні; – асиметричні; – функції гешування; – функції генерування та перевірки таємних та відкритих парамет-рів	– симетричні; – асиметричні; – функції гешування; – функції генерування та перевірки таємних та відкритих параметрів
2) Види протоколів	– встановлення ключа; – автентифікації; – розподілу спільної таємниці; – вироблення ключа; – обміну; – управління ключовими данними;	– встановлення ключа; – автентифікації; – розподілу спільної таємниці; – вироблення ключа; – обміну;
3) Застосуван-ня протоколів	– програмне забезпечення для аутентифікації, ідентифікації ключів та абонентів; – програмне та апаратне забезпечення конфіденційності, цілісності даних; – розподілення секретів в системах безпеки (протоколи для систе-ми безпеки p2p, Grid Computing); – забезпечення безпеки в групах (в програмах орієнтованих на роботи в групах, та корпоративних мережах); – електронна торгівля (оплати послуг та товарів); – онлайн-банкінг (за допомогою мережі Internet та/або терміналів); – програмне забезпечення для апаратних комплексів, що використовуються для «Довірених обчислень»; – мережева безпека (безпека в середовищах Internet, WAN,WLAN,LAN); – забезпечення безпеки мобільної мережі; – вільне та відкрите ПЗ (OpenPGP); – IP Security Protocol (IPSec) – дистанційне керування доступом та IP-безпека віддаленого досту-пу (ipsra); – виявлення вторгнень; – вироблення ключів в середовищі Internet (kink); – державна інфраструктура відкритих ключів (X.509) та проста інфраструктура відкритих ключів (SPKI); – захист електронної пошти (SMIME); – безпечний протокол мітки часу (STIME); – забезпечення безпеки на транспортному рівні (Transport Layer Security (TLS)); – Веб-безпека транзакцій (wts); – XML цифровий підпис; – національна система; – малі платіжні системи та термінали; – системи електронної готівки та електронних чиків; – електронного документообігу; – електронний уряд.	– програмне забезпечення для ау-тентифікації, ідентифікації ключів та абонентів; – програмне та апаратне забезпечення конфіденційності, цілісності даних; – програмні та апаратні комплекси для розподілення спільних секретів в системах; – мережева безпека (безпека в середо-вищах Internet, WAN,WLAN,LAN); – IP Security Protocol (IPSec); – електронного документообігу; – малі платіжні системи та термінали; – інфраструктура відкритих ключів;
4) Види атак на протоколи:	Атаки на сам протокол: – повтор раніше переданого повідомлення; – маскарад; – віддзеркалення; – на криптографічний примітив; Атаки на його реалізацію: – переповнення буферу пристроя; – помилки при реалізації чи конфігурації обладнання; – ненадійність середи функціонування; – атаки на рівні ядра.	Атаки на сам протокол: – повтор раніше переданого повідом-лення; – маскарад; – віддзеркалення; – на криптографічний примітив; Атаки на його реалізацію: – переповнення буферу пристроя; – помилки при реалізації чи конфігура-ції обладнання; – ненадійність середи функціонування; атаки на рівні ядра.
5) Стандарти протоколів	ISO/IEC 9796-2:2002 ISO/IEC 9796-3:2006 ISO/IEC CD 9797-1 ISO/IEC CD 9797-2 ISO/IEC WD 9797-3 ISO/IEC FDIS 9798-2 ISO/IEC CD 9798-5 ISO/IEC 11770-2:2008 ISO/IEC 11770-3:2008 ISO/IEC 11770-4:2006 ISO/IEC 15946-1:2008 ISO/IEC CD 15946-5 ISO/IEC FCD 19772 ISO/IEC WD 29128 ISO/IEC NP 29146 ISO/IEC TR 14516:2002	ISO/IEC 9796-2:2002 ISO/IEC 9796-3:2006 ISO/IEC CD 9797-1 ISO/IEC CD 9797-2 ISO/IEC WD 9797-3 ISO/IEC FDIS 9798-2 ISO/IEC CD 9798-5 ISO/IEC 11770-2:2008 ISO/IEC 11770-3:2008 ISO/IEC 11770-4:2006 ISO/IEC 15946-1:2008 ISO/IEC CD 15946-5 ISO/IEC FCD 19772 ISO/IEC WD 29128 ISO/IEC NP 29146 ISO/IEC TR 14516:2002

Продовження табл. 6

Критерій	Німеччина	Україна
6) RFC протоколів	Група X9 – Фінансові сервіси. – X9.30: Part 3: Управління сертифікатами – X9.42: Узгодження ключів Діффі-Гелмана – X9.44: Транспортування ключів з використанням RSA – X9.41: Механізм управління сервісами безпеки Група RSA DSI – PKCS #3: Узгодження ключів Діффі-Гелмана – PKCS #7: Синтаксис криптографічних повідомлень Група ECMA: European Computer Manufacturers Association – ECMA-205, Commercially oriented functionality class for security evaluation (COFC), 1st Edition (December 1993)	

ВИСНОВКИ

Результати аналізу та порівняння криптографічних систем України та Німеччини дозволили зробити висновок, що національний банк Німеччини суттєву увагу приділяє впровадженню найбільш перспективних криптографічних примітивів. Німеччина не використовує власної криптографії, а користується міжнародними стандартами. Це дозволяє налагоджувати тісну співпрацю цієї держави з іншими державами світу в різноманітних сферах. Негативним є те, що Німеччина дозволяє використовувати TDES, що не відповідає сучасним вимогам. Але національні стандарти Німеччини BSI вказують шифри, що забезпечують задовільний рівень захищеності. На основі проведеного аналізу були визначені вимоги до можливих строків та умов застосування асиметричних криптографічних перетворень для захисту банківської інформації в Німеччині, а також використання строків та умов в Україні.

Стосовно України можна зробити висновок, що Україна має суттєві досягнення, але відстає в темпах впровадження визнаних міжнародних стандартів, таких як ISO/IEC 9796, ISO/IEC 15946- 2, ISO/IEC 1488 -3, ISO/IEC 18031 та ISO/IEC 18033 тощо. Якщо Україна реально впровадить для захисту банківської інформації симетричні шифри згідно ISO 18033-3,4, а на національному рівні – шифр Калина, то рівень захищеності банківської інформації буде відповідати самим високим міжнародним вимогам.

Одним із способів вирішення питання взаємодії банків різних держав є розділення криптографії на комерційну та державну. Комерційна криптографія повинна засновуватися на однакових стандартах для всього світу, бо сучасний бізнес, а тим паче банківський сектор, часто виходить за рамки окремої держави. Державні ж стандарти криптографічного захисту повинні використовуватися лише для забезпечення потреб держави, а саме для збереження державної таємниці, та оновлюватися з певною періодичністю, в встановлені строки державою.

Література.

[1] http://www.cryptool.org/

[2] http://www.bsi.bund.de/

[3] The IT Security Situation in Germany in 2009, Federal Office for Information Security.

[4] Security Considerations with Electronic Commerce, BSI series on IT security, 2007.

[5] ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Крипто-графическая защита информации. Функция хеширования. Киев. Госстандарт Украины. 1998.

[6] ГОСТ 28147-89 Информационная технология. Криптографическая защита информации. Симметрические алгоритмы шифрования. Киев. Госстандарт Украины. 1989.

[7] ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України, 2003.

[8] ISO/IEC 18033-2,3,4 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, Part 3: Block ciphers, Part 4: Stream ciphers, 2005.

[9] ISO/IEC 14888-1,2,3: Information technology – Security techniques – Digital signatures with appendix, 2006.

[10] *Горбенко И.Д.* Отчет по результатам разработки и исследования симметричного блочного алгоритма шифрования «Калина» – спецификация алгоритма «Калина» / И.Д. Горбенко, В.И. Долгов, Р.В. Олейников и др., // Х.: ЗАО «ИИТ», 2007.

[11] *Аулов І.Ф., Кутя Є.Ю., Хряпін Д.Е.* Порівняльний аналіз криптографічних систем національних банків України та Німеччини. //Труды научно-технической конференции КМНТ, часть 1, 2010.

[12] NIST: FIPS Publication 186-3: Digital Signature Standard, June 2009.

[13] ISO/IEC 10118-3 Information technology — Security techniques — Hash-functions

Надійшла до редколегії 18.06.2010.

Горбенко Юрій Іванович, канд. техн. наук, технічний директор ЗАТ «ІІТ». Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

Аулов Іван Федорович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження принципів побудування, розгортання та аналізу стійкості криптографічних систем, заснованих на ідентифікаторах.

Кутя Євген Юрійович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: аналіз асиметричних криптосистем і хеш-функцій, асиметричні криптопримітиви в групі точок еліптичних кривих.

Хряпін Дмитро Едуардович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: криптоаналітичні властивості БСШ, симетричні криптосистеми та протоколи.

УДК 004.056:[336.71(430)+336.71(477)]

Сравнительный анализ криптографических систем национальных банков Украины и Германии / Ю.И. Горбенко, И.Ф. Аулов, Е.Ю. Кутя, Д.Э. Хряпин // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 404-410.

Приводятся результаты анализа и сравнения криптографических примитивов, применяемых и планируемых к применению для защиты информации в банковских информационных технологиях Украины и Германии.Определен перечень стандартов, предлагается к внедрению и применению на территории Украины.

Ключевые слова: криптографические системы, криптографические примитивы.

Табл. 06. Библиогр.: 05 назв.

UDC 004.056:[336.71(430)+336.71(477)]

Comparative analysis of cryptographic systems of national banks of Ukraine and Germany / Yu.I. Gorbenko, I.F. Aulov, E.Yu. Kutya, D.A. Hryapin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 404-410.

The results of analysis and comparison of cryptographic primitives used and planned to be used for information protection in bank information technologies of Ukraine and Germany are given. A list of standards is determined which is proposed for implementation and use in Ukraine.

Key words: cryptographic systems, cryptographic primitives.

Tab. 06. Ref.: 05 items.