УДК 004.056.53

Нємкова О. А.

ШЛЯХИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНТЕРНЕТ-БАНКІНГУ

У статті проаналізовано причини існування кіберзлочинності у сфері надання дистанційних банківських послуг населенню. Розглянуто питання підвищення безпеки інтернет-банкінгу завдяки впровадженню взаємної двофакторної автентифікації. У якості факторів запропоновано використовувати пін-код і токен. Запропоновано алгоритм генерації хеш-функції для проведення автентифікації, а також протокол взаємної автентифікації за допомогою згенерованої хеш-функції. Дані біометрики можуть слугувати сеансовим ключем.

Ключові слова: *інтернет-банкінг, двофакторна автентифікація, кіберзлочинність, фішинг, токен, біометрика, протокол автентифікації.*

В статье проанализированы причины существования киберпреступности в сфере дистанционных банковских услуг населению. Рассмотрены вопросы повышения безопасности интернет-банкинга вследствие использования взаимной двухфакторной аутентификации. В качестве факторов предложено использовать пин-код и токен. Предложен алгоритм генерации хеш-функции для проведения аутентификации, а также протокол взаимной аутентификации с помощью сгенерированной хеш-функции. Данные биометрики могут быть использованы в качестве сеансового ключа.

Ключевые слова: *интернет-банкинг, двухфакторная аутентификация, киберпреступность, фишинг, токен, биометрика, протокол аутентификации.*

The reasons for the existence of cybercrime in remote banking services for the public have been analyzed in the article. The questions of a more secure Internet banking through the use of mutual two-factor authentication have been considered. There is proposed to use a PIN and token as the factors. The algorithm for generating the hash function to provide authentication have been proposed, as well as the protocol of mutual authentication by using a hash function. This biometrics may be used as a session key.

Key words: *Internet banking, two-factor authentication, cybercrime, phishing, token, biometrics, authentication protocol.*

Постановка проблеми. Усебічне проникнення інформаційних технологій у будь-який вид діяльності людства викликає проблему забезпечення інформаційної безпеки. У наш час питання безпеки порушуються практично в будь-якій галузі, починаючи від харчової промисловості та медицини і закінчуючи інформаційно-комунікаційними системами. Особливо це стосується економіки, а в економіці – банківської галузі.

Одним зі способів надання більшості населення банківських послуг є інтернет-банкінг, зручність якого полягає в можливості користуватись ним у будь-який час доби практично в будь-якому місці. В інтернет-банкінгу велика частина інформаційної безпеки покладається на плечі самого користувача. Аналіз ситуації показує, що на сьогодні користувач не в змозі забезпечити собі надійну інформаційну безпеку. Це є причиною існування різноманітних способів шахрайських дій по відношенню до карткових рахунків.

Основними трендами безпеки платіжних систем є протидія кібератакам і фішингу. Кібератаки спрямовані в основному на програмно-апаратне забезпечення. Фішинг цілком і повністю орієнтується на людину і є породженням соціальної інженерії. Таким чином, при найбільш відповідальних моментах роботи з платіжною системою, тобто проведенні входу в платіжну систему, а також підтвердженні правильності транзакції будуть виникати моменти, які кіберзлочинці намагаються взяти під контроль.

Основною проблемою при реєстрації користувача в платіжній системі є проблема його автентифікації. Історично потреба в суворій автентифікації виникла через людський фактор – людина не в змозі запам'ятати надійний пароль, який за короткий час не можна було б підібрати за допомогою програм брутфорсу. Тоді було запропоновано інший фактор автентифікації, який спирався на те, що людина має якусь річ, яка

однозначно її характеризує. Такою річчю може бути пластикова картка з чіпом для роботи з платіжною системою або пластикова картка із вбудованим у неї магнітним ключем для проходу в приміщення з обмеженим правом входу та ін. Подальше посилення автентифікації пов'язано з тим, що людина собою являє біометричну інформацію. Але зрозуміло, що недбалість по відношенню до факторів автентифікації нівелює всі їх переваги. Усе це відбувається завдяки наявності слабкого місця в системі захисту – людини. Це дуже добре відомо злочинцям, які використовують методи соціальної інженерії.

Надійної автентифікації користувача при роботі в інтернет-банкінгу до цього часу немає. Двофакторна автентифікація є надійною тільки в ідеалі. Розглянемо більш детально особливості двофакторної автентифікації користувачів інтернет-банкінгу.

Перший фактор є тим, що людина знає – пароль. Як правило, придумати та запам'ятати надійний пароль для кожного сервісу практично неможливо для більшості користувачів платіжних систем. Спостерігається така тенденція: використання одного й того ж пароля для різноманітних задач – для електронної пошти, інтернет-банкінгу, входу в профіль на домашньому та робочому комп'ютері та ін. Знаючи це, кіберзлочинець буде намагатися знайти слабке місце на одному з комп'ютерів. Нескладно здогадатись, що таким місцем буде домашній комп'ютер, на якому не такий сильний захист, як на робочому комп'ютері. До того ж, як правило, операційна система Windows на домашньому комп'ютері ставиться з виключеними сервісами мережевого захисту, а антивірусний продукт, якщо і встановлений, то з обмеженими можливостями. Ще декілька років тому за статистикою на кожному персональному комп'ютері «жило» десь 240 програм, установлених ззовні без відома його господаря. Тому навчити створювати надійні паролі для кожного сервісу є одним із завдань надійної автентифікації. Перед користувачем же, як правило, ставиться лише завдання створення довгого пароля, але ніде не знайти зауваження, що пароль для кожного сервісу повинен бути унікальним.

Другий фактор є тим, що людина має. Як правило, у країнах СНД таким предметом вважається мобільний телефон. На нього зручно надсилати смс-повідомлення, які являють собою таємний код для входу в інтернет-банкінг чи підтвердження трансакції. Зазвичай, недовготривалість валідності надісланого смс-коду дещо підвищує безпеку. Але мобільний телефон не є настільки надійним у принципі, щоб довіряти йому таємниці банківського рахунку. Втрата мобільного телефону, як правило, асоціюється зі втратою великої кількості контактних даних, а не виникненням проблем із власним рахунком, яким користувач керує за допомогою цього пристрою. Ставлення до власного мобільного телефону достатньо недбале – його носять у зовнішніх кишенях верхнього одягу, можуть забути в кафе та ін. До цього можна додати, що завжди, маючи свій мобільний при собі, користувач не може бути впевненим у безпеці інтернет-банкінгу, тому що сучасні технології дозволяють переспрямовувати смс-повідомлення на інший номер, або організувати дублікат сім-карти.

У своїй відомій книзі «Мистецтво обману» Кевін Митник назвав шість факторів соціальної нестійкості людини [1]. По відношенню до інтернет-банкінгу та пов'язаних із ним схем фішингу можна відібрати дві: прагнення підкорятись авторитету та відповідальність. Отримавши вказівку нібито від серверу банку, а насправді від злочинця, ввести в поля форми свої автентифікаційні дані, середньостатистичний користувач із відчуттям добре виконаної відповідальної роботи вводить їх із відомим надалі результатом – пароль потрапляє в руки кіберзлочинцям. Треба зауважити, що при спілкуванні з працівниками банку майже ніколи не можна почути застереження про те, що за жодних умов банк не буде запитувати в користувача його автентифікаційну інформацію. Говорять інші слова на кшталт того, що при першому вході в систему інтернет-банкінгу рекомендується змінити пароль. Зрозуміти таку позицію можна, тому що подібні розмови можуть налякати недосвідчену людину та відбити всіляке бажання користуватись інтернет-банкінгом. В основному, про можливі негаразди з інтернет-банкінгом, а саме про фішинг та кіберзлочинність, користувач дізнається з інтернету (соціальні мережі) або при спілкуванні зі знайомими.

Схема двофакторної автентифікації мала б добре спрацьовувати, як би не фактори соціальної нестійкості. Потрібно нівелювати ці фактори шляхом зменшення ролі користувача та переносу акценту на автоматизацію процедури автентифікації, яка до того ж має бути взаємною.

Таким чином, теоретично достатньо безпечну двофакторну автентифікацію, завдяки порушенням, пов'язаним із особливостями поведінки середньостатистичного користувача, кіберзлочинець може легко обійти. Велика кількість крадіжок із рахунків, що обслуговуються інтернет-банкінгом, підтверджує цей висновок.

Аналіз останніх досліджень та публікацій. Європейська практика проведення онлайнових банківських платежів свідчить про різноманітність автентифікаційних методів: ідентифікаційний код клієнта плюс пароль/пін-код із наступним введенням TAN (номер трансакції). TAN може бути використаний тільки один раз. Найбільш часто використовувані TAN варіанти є такими [2-5]:

– мобільні TAN (повідомлення надсилається на мобільний телефон клієнта; використовується в Австрії, Болгарії, Грецькій республіці, Німеччині, Нідерландах, Польщі, Росії, Україні, Угорщині, Швейцарії, Нової Зеландії, Австралії);

– iTAN (проіндексовані TAN);

– класичні TAN – банк попередньо видає клієнту надрукований перелік номерів для одноразового використання;

– сiTAN – чіп TAN. Використовуються більшістю банків Німеччини. Генерація відбувається за допомогою чіп-картки;

– токенTAN або фотоTAN. Працюють за використанням QR – кодів.

Європейські рекомендації для безпечних інтернет-платежів, що прийняті в січні 2013 р. Європейським центральним банком [6], містять 14 рекомендацій, або ключових факторів. Ці фактори описують політику безпеки, оцінку ризиків, правила моніторингу інцидентів та звітності, можливості нагляду інцидентів, початкову ідентифікацію клієнта, сильну автентифікацію, вимоги до програмного забезпечення та інструменти автентифікації, моніторинг трансакцій, забезпечення доступу клієнта до інформації про стан рахунку.

В останні роки в Україні з'явилося багато досліджень, присвячених інформаційній безпеці віддаленого доступу, особливо в банківський галузі. Частина цих досліджень увійшла до сучасних підручників. Можна відзначити роботи Харківської, Київської та Львівської шкіл, які розглядають питання побудови та супроводження комплексних систем санкціонованого доступу, міжнародні нормативні документи, що діють в Україні та за її межами [7-10].

Формулювання цілей статті. Цілями статті є розгляд можливого алгоритму формування хеш-функції на базі кількох факторів, оцінка її стійкості до брутфорсу та опис протоколу взаємної автентифікації на базі даної хеш-функції. Основною вимогою до хеш-функції, яка є важливою при застосуванні для даного протоколу, виступає стійкість до загального типу атак, а також її статистичні властивості. Вимога ж на швидкодію у цьому випадку не настільки важлива.

Виклад основного матеріалу дослідження. Для посилення автентифікації потрібно мінімізувати фактори соціальної нестійкості в тому, що стосується другого фактору автентифікації – що користувач має. Мобільний телефон у наш час має багато призначень, окрім телефонних розмов та надсилання смс-повідомлень, і не є предметом суворого контролю зі сторони його власника. Роль предмета, який користувач має для роботи з інтернет-банкінгом, може відігравати спеціальний токен – електронний ключ, який видається користувачу в банку для авторизації та підтвердження трансакцій у платіжній системі. Ставлення до такого токену буде особливим і зовсім не таким недбалим, як до мобільного телефону, завдяки факторам соціальної нестійкості – підкорення авторитету та відповідальності. Тільки на цей раз фактори будуть «грати на руку» безпеці. Якщо працівник банку зауважить, що при акуратному ставленні до токену та збереженні його вдома у відповідно безпечному місці ризик крадіжки зводиться до нуля, користувач буде виконувати цю пораду зі всією відповідальністю. Використання токену дозволить ускладнити процедуру автентифікації, яка, без сумніву, підвищить безпеку трансакцій – систему одноразових паролів і взаємну автентифікацію. Таким чином, можна буде запобігти різноманітним фішинговим схемам зі введенням парольної інформації – людина просто не буде знати пароля.

По-друге, потрібно дещо змінити у вивченні дисциплін, що пов'язані з безпекою банківської діяльності. У першу чергу, потрібно показати можливий захист найслабшого місця у спілкуванні людини з інформаційною системою – це протизахист від атак соціальної інженерії. Не так важливо знати механізм захисту в деталях (різноманітні схеми на кшталт Диффі-Хелмана чи шифрування на еліптичних кривих та ін.), як знати про існування цього захисту та його надійність. Важливо ввести в обов'язок банківських працівників більш детальні роз'яснення щодо правил безпеки користування інтернет-банкінгом.

Зменшення фактору соціальної нестійкості може бути розв'язано через удосконалення протоколу автентифікації. Вимоги до автентифікації повинні бути такими:

– автентифікація має бути двофакторною;

– фактори автентифікації мають взаємодіяти між собою;

– обробка факторів автентифікації має вестись не комп'ютером користувача, який може бути заражений різноманітними шкідливими програмами, а токеном, який має бути програмно захищений від проникнення в нього шкідливих програм.

Розглянемо алгоритм утворення хеш-функції, яку можна запропонувати для задач автентифікації клієнта у інтернет-банкінгу. Довжина хеш-функції дорівнює 256 байт. Для роботи алгоритму потрібний генератор псевдовипадкових чисел, причому над послідовністю у процесі роботи алгоритму виконується операція ділення по модулю на 16, що є незворотним криптографічним примітивом. Тому у якості генератора можна взяти, наприклад, лінійний конгруентний генератор. Відомо, що для роботи такого генератора потрібно чотири числа: початкове значення послідовності a_0, та числа b, c, m. Тоді наступний член послідовності a_n можна записати як $a_n = (ba_{n-1} + c) mod\ m$. Числа b, c, m повинні бути взятими з рекомендованого переліку Національного бюро стандартів США для отримання послідовності з гарними статистичними властивостями [11].

Розглянемо таблицю 16×16. Нехай i – нумерація рядків, а j – нумерація стовпців. Для запису величин i та j потрібно по 4 біти. Елемент таблиці приймемо рівним $p_{ij} = ij$, тобто у правий півбайт записується значення величини i, а у лівий півбайт-значення величини j. Таким чином, таблиця P_0 набуває вигляду (запис наведено у шістнадцятковій системі числення), рис. 1.

00	01	02	…	0E	0F
10	11	12	…	1E	1F
20	21	22	…	2E	2F
…	…	…	…	…	…
E0	E1	E2	…	EE	EF
F0	F1	F2	…	FE	FF

Рис. 1. Початковий стан таблиці хеш-функції P_0

Операції, що виконуватимуться над початковою таблицею P_0, будуть складатись із циклічних зсувів рядків та стовпців. Величина зсуву буде визначатись або за формулою $z_n = a_n \ mod16$, або формуватись із даних, які вносить користувач, та мітки часу. Черговість рядків або стовпців при зсуві визначатиметься парністю чи непарністю цифр послідовності z_n. Таким чином, кожен рядок чи стовпець буде циклічно зсунутий на іншу величину. Для надійного перемішування елементів таблиці потрібно виконати щонайменше 32 зсуви.

Кожен користувач повинен зареєструватись у банку особисто, щоб отримати токен для роботи в інтернет-банкінгу та значення піну. Зауважимо, що у цьому випадку пін-код не є особистою інформацією користувача, його повинен знати також банк. Надалі пін-код буде використовуватись із метою ідентифікації користувача. Для кожного користувача має бути своя індивідуальна таблиця P. Досягти цього можливо шляхом введення ним при очній реєстрації в банку фрази чи просто послідовності символів довжиною не менш ніж 32 символи. Символи вводяться один раз, запам'ятовувати їх не потрібно. Кожний символ задає величину циклічного зміщення рядка, якщо відповідне число символу за таблицею ASCII є парним, та стовпця, якщо непарним. Першим виконується зсув рядка чи стовпця, номер якого співпадає з номером символу за модулем 16. Надалі циклічні зсуви виконуються за порядком зростання номерів, чергуючи рядок та стовпець. Звичайно, ті правила можна змінити, головне, щоб випадковими були номер рядка чи стовпця, з якого починається цикл зсувів. Таблиця перестановок, що утворилась при виконанні перемішування, вважається таблицею ініціалізації.

Наступним кроком алгоритму є циклічні зсуви рядків та стовпців, які виконуються аналогічно, що при утворенні таблиці ініціалізації, тільки величина зсувів визначається послідовністю z_n. Метою перемішування є покращення статистичних характеристик таблиці. За один цикл перемішування виконується 32 операції зсувів.

На виході після одного циклу перемішування виходить таблиця, яка є основою криптографічного перетворення даних, що надходять від користувача в процесі авторизації. Ця таблиця зберігається в користувача в токені та в процесинговому центрі банку. Тобто користувача характеризує пін-код, таблиця $P_{\text{пк}}^{K}$ – значення хеш-функції та послідовність a_n.

Оцінімо стійкість такої хеш-функції до брутфорсу. Кількість варіантів різних таблиць складатиме 64!, при підрахунку за формулою Стирлінга $\approx 10^{89}$. При частоті процесора 10^{10} Гц потрібно $\approx 10^{70}$ років, щоб виконати хоча б по одному такту комп'ютера на одну таблицю. Набагато меншою є довжина псевдовипадкової послідовності лінійного конгруентного генератора. При відповідному виборі параметрів період такої послідовності може бути 2^{35}, що в переведені на роки роботи процесора складає 1 090 років. Згадуючи, що значення генерованої таблиці активне впродовж кількох секунд, доки не пройдена взаємна автентифікація (або сесія), зрозуміло, що при нинішньому стані обчислювальної техніки запропонована схема стійка до брутфорсу.

Спілкування користувача із системою інтернет-банкінгу має бути неможливим без токену. При взаємній автентифікації користувача та системи активною стороною виступає користувач-клієнт, який при підключенні вводить у програму значення пін-коду, до якого автоматично під'єднується дата звернення і доповнюється до довжини 32 байти наступними членами послідовності z_n. Відбувається цикл зсувів за описаним вище алгоритмом. Далі певним чином визначена половина таблиці $P_{\text{пк}}^{KI}$ (тільки парні чи непарні рядки, або верхня половина таблиці, або ті елементи таблиці, сума чиїх номерів парна чи непарна та ін.) відправляється до процесингового центру разом із пін-кодом. Отримавши пін-код (ідентифікатор користувача) та частину таблиці, процесинговий центр виконує аналогічні перетворення з таблицею користувача, що зберігається в центрі та порівнює визначену половину своєї таблиці $P_{\text{пк}}^{BI}$ із надісланою половиною таблиці користувача. Якщо дані не збігаються (наприклад, неправильно введений пін-код, або не справжній користувач), то з процесингового центру надсилається повідомлення, що авторизація не пройдена, відбувається відкат даних таблиці $P_{\text{пк}}^{K}$ та псевдовипадкової послідовності до попереднього стану. Авторизація відбувається знову за умови повторного введення пін-коду. Якщо дані збігаються, то центр надсилає користувачу решту таблиці $P_{\text{пк}}^{BII}$, яка порівнюється з частиною таблиці користувача $P_{\text{пк}}^{KII}$. При збігу даних взаємна авторизація вважається підтвердженою, про що токен має надіслати код підтвердження. Якщо дані не збігаються, токен не підтверджує взаємну автентифікацію, до процесингового центру надсилається код відкату на попереднє значення даних. Графічну схему взаємної двофакторної авторизації наведено на рис. 2.

Клієнт-користувач	Банк-процесинговий центр
P_{n-1}^{K}	P_{n-1}^{B}
Початок нової сесії	
Введення пін-коду. Генерація P_n^K	
Передача пін-коду, P_n^{KI}	
	Генерація за надісланим пін-кодом P_n^B
	Порівняння P_n^{KI} та P_n^{BI}
Відкат до P_{n-1}^{K}	Неспівпадіння. Співпадіння Відхилення процедури. Передача P_n^{BII} автентифікації Відкат до P_{n-1}^{B}
Порівняння P_n^{KII} та P_n^{BII}	
Неспівпадіння. Співпадіння, надсилання коду, співпадіння Відхилення процедури автентифікації Відкат до P_{n-1}^{K} Передача коду відхилення	Отримання коду співпадіння **Успішне завершення** **автентифікації** Відкат до P_{n-1}^{B}

Рис. 2. Протокол взаємної автентифікації за допомогою згенерованої хеш-функції

Відмітимо, що ця таблиця дозволяє також шифрувати відкриті ключі у схемах асиметричного шифрування для запобігання атаки типу «людина посередині».

Висновки дослідження і перспективи подальших розвідок у цьому напрямі. Проведене дослідження показало, що існує можливість генерації хеш-функції у вигляді спеціальної таблиці перестановок, яка забезпечує криптографічне закриття параметрів взаємної автентифікації і має достатню стійкість для використання в онлайнових платежах.

Дуже перспективним напрямом слід вважати використання біометрик для посилення протоколу автентифікації. У деяких ноутбуках передбачено використовувати відбиток пальця для можливості доступу до інформації тільки господаря ноутбука. У наш час активно починає застосовуватися біометрика малюнка судин долоні в банкоматах. Такі банкомати з'явились уже в Японії, Польщі. Таким чином, можна доукомплектувати власний комп'ютер таким пристроєм, який би зчитував біометрику людини та записував би ці дані не в сам комп'ютер, а в токен, також підключений до комп'ютера. Зауважимо, що передавати біометричні дані у відкритому вигляді не можна, до того ж доцільно комбінувати їх за допомогою певного криптографічного протоколу з даними попереднього значення хешу. Фактично послідовність даних біометрики буде визначати величини зсувів рядків та стовпців у таблиці хеш-функції. У такий спосіб відбудеться об'єднання факторів автентифікації.

Створення системи взаємної сильної авторизації в інтернет-банкінгу забезпечує надійність проведення он-лайн платежів. У такий спосіб можна підвищити довіру населення до користування інтернет-банкінгом, відповідно збільшивши кількість клієнтів та зменшивши збитки банку від повернення незаконно списаних грошей із рахунків клієнтів.

ЛІТЕРАТУРА

1. Митник К. «Искусство обмана» [Електронний ресурс] / Кевин Митник. – Режим доступу : http://www.evartist.narod.ru/text16/033.htm.
2. Heise online (2007-10-26) «Verbessertes iTAN-Verfahren soll vor Manipulationen durch Trojaner schützen» (in German).
3. Li, Shujun; Syed Amier Haider Shah, Muhammad Asad Usman Khan, Syed Ali Khayam, Ahmad-Reza Sadeghi and Roland Schmitz (2010). «Breaking e-Banking CAPTCHAs». Proceedings of 26th Annual Computer Security Applications Conference (ACSAC 2010). New York, NY, USA: ACM. pp. 171–180.
4. Postbank chipTAN comfort, official page of Postbank.
5. ChipTAN: Listen werden überflüssig, official page of Sparkasse.
6. Http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf?7f72ee8a86c6443f25239149b65d644c.
7. Засадна Х. О. Про захист послуг інтернет-банкінгу / Х. О. Засадна // Вісник Університету банківської справи Національного банку України. – № 3. – 2008. – С. 225–229.

8. Гарасимчук О. І. Комплексні системи санкціонованого доступу : [навч. посіб.] / О. І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака. – Львів : Видавництво Львівської політехніки, 2010. – 212 с.
9. Горбенко І. Д. Прикладна криптологія: Теорія. Практика. Застосування : [підручник для вищих навчальних закладів] / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2013. – 880 с.
10. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.
11. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : «Триумф», 2002. – 520 с.

 Дата надходження статті до редколегії 05.10.2013 р.

НЄМКОВА Олена Анатоліївна – кандидат фізико-математичних наук, доцент кафедри економічної кібернетики, Університет банківської справи Національного банку України, м. Київ, Львівський інститут банківської справи, м. Львів.

Коло наукових інтересів: протоколи автентифікації, стеганографічні методи захисту інформації, генератори псевдовипадкових послідовностей, криптографічні алгоритми.