УДК 004.725.5

АНАЛІЗ ДІЮЧИХ ПРОТОКОЛІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЕЛЕКТРОННИХ ТРАНЗАКЦІЙ

ЙОНА Л. Г., КЮНЕ О.О.

Одеська національна академія зв'язку ім. О.С. Попова,
вул. Кузнечна, 1, Одеса, 65029, Україна
lyona@list.ru

АНАЛИЗ ДЕЙСТВУЮЩИХ ПРОТОКОЛОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ЭЛЕКТРОННЫХ ТРАНЗАКЦИЙ

ЙОНА Л. Г., КЮНЕ Е.О.

Одесская национальная академия связи им. А.С.Попова,
ул.Кузнечная, 1, Одесса, 65029, Украина
lyona@list.ru

ANALYSIS OF ACTIVE CRYPTOGRAPHIC PROTOCOLS FOR PROTECTION OF ELECTRONIC TRANSACTIONS

YONA L. G., KUEHNE O. O.

O.S. Popov Odessa national academy of telecommunications
Kuznechna st., 1, Odessa, 65029, Ukraine
lyona@list.ru

Анотація*. У статті розглядаються дійсні протоколи захисту електронних транзакцій, зокрема, SSL,SET, OBI, OFX, IOTP, 3-DSecure.Розглянуто особливості наданих протоколів та зроблено висновки щодо стану сучасних технологій захисту електронних транзакцій.*

Ключові слова*:криптографічний захист електронних транзакцій, Інтернет – еквайринг ,технологія SET, технологія 3-DSecure.*

Аннотация*.В статье рассматриваются действующие протоколы защиты электронных транзакций, в том числе, SSL,SET, OBI, OFX, IOTP, 3-DSecure. Рассмотрены особенности приведённых протоколов и сделаны выводы относительно состояния современных технологий защиты электронных транзакций.*

Ключевые слова*: криптографическая защита электронных транзакций, Интернет–эквайринг, технология SET, технология 3-D Secure.*

Abstract*. The article deals with the current protocols for the protection of electronic transactions, including SSL, SET, OBI, OFX, IOTP, 3-D Secure. The features of these protocols are considered and conclusions are made regarding the state of modern technologies for the protection of electronic transactions.*

Key words*: protection of electronic transactions payment systems, Internet - acquiring, SET technologies, 3-D Secure technology.*

Будь-який вид розрахунків за допомогою мережі Інтернет (оплата послуг, покупка або продаж товару чи інформації) потребує легкого універсального способу, який дозволяв би здійснювати зручні, дешеві, швидкі та безпечні електронні транзакції в режимі реального часу.

Технології здійснення електронних платежів постійно розвиваються. Так,на сьогоднішній день число людей, що здійснюють покупки через Інтернет, перевищила мільярд! Незважаючи на постійне зростання шахрайства, зручність і швидкість здійснення розрахунків за допомогою мережі Інтернет веде до збільшення користувачів Інтернет-еквайрингу. При цьому важливе виконання двох умов: забезпечення необхідного рівня сервісу і гарантування безпеки для всіх учасників процесу здійснення платежів за допомогою пластикової картки через мережу Інтернет,що потребує використання сучасних методів захисту електронних транзакцій. Технології захисту інформації під час Інтернет - еквайрингу також стрімко розвиваються, то-

му є необхідність подальшого дослідження цього питання з метою удосконалення протоколів захисту [1-4].

Захист віддалених банківських транзакцій є актуальним питанням й існує значна кількість методів їх захисту. Проте одним із найнадійніших засобів захисту інформації є використання криптографічних протоколів.

За допомогою криптографічних протоколів вирішуються різноманітні завдання, а саме: захист інформації шляхом шифрування; підтвердження дійсності користувача/документа за допомогою протоколів автентифікації; розподілення ключів.

Проблемам дослідження методів захисту інформації в електронних платіжних системах присвячені праці багатьох вчених, включаючи зазначених в [1–16]. Так, у [1] класифікуються за призначенням методи криптографічного захисту документообігу. У [2]розглянута проблема забезпечення безпеки електронних платежів. Проблемам дослідження методів захисту інформації в локальних мережах банку присвячено [3]. Питання забезпечення безпеки інформації при використанні пластикових карток за допомогою технології 3-D Secure обговорюються в [4]. У [5] розглядається розподілена система виявлення шахрайських платежів. Протокол захисту електронних платежів 3-D Secure описується у [6]. Сучасні принципи побудови захищених інтелектуальних мереж, які можуть використовуватися у системах забезпечення економічної безпеки та організація процесу розробки програмного забезпечення для них, розглядаються у [7]. У [8] відзначені специфічні чинники, які підсилюють активізацію загроз економічній безпеці господарюючих суб'єктів. У[9] зроблена систематизація типових моделей загроз безпеці персональних даних, які обробляються у спеціальних інформаційних системах підприємств. У[10] розглянуто новий предмет інформаційних правовідносин - відомості щодо наданих людині телекомунікаційних послуг, які водночас опрацьовано в ролі предмета інформаційної безпеки людини як споживача телекомунікаційних послуг. Запропоновано нову модель забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг. У[11] описуються кіберстандарти безпеки і промислового застосування : системи та методології. У[12] розглядаються принципи, методи та програми ситуаційної обізнаності в комп'ютерній мережі, що захищається. У[13]розглядаються технології захисту інформації в електронних платіжних системах та надано класифікацію систем електронних платежів. У[14]розглядається захист електронних транзакцій в платіжних системах, зокрема, рішення на базі технологій SET и 3-D Secure, перелічені переваги та недоліки наданих технологій. У[15;16]розглядаються протоколи електронної комерції. Проте, у вищезазначених роботах не надається аналіз діючих криптографічних протоколів захисту.

Аналіз сучасних технологій захисту електронних транзакцій, виявлення та усунення недоліків протоколів підвищить безпеку транзакцій під час Інтернет –еквайрингу. Тому з метою удосконалення технологій захисту електронних транзакцій є необхідність подальшого дослідження цього напрямку.

Існує багато різних електронних платіжних систем, серед них Visa, MasterCard, EasyPay, Portmone, iPay та інші. Корпорації Visa та MasterCard для того, щоб підвищити безпеку і захищеність електронних платежів постійно використовують останні досягнення науки, розробляють інноваційні рішення на основі даних і аналітичних висновків, залучаються передові технології. Так, платіжними системами Visa і MasterCard були розроблені протоколи захисту на базі технологій SET и 3-DSecure.

Метою дослідження є визначення стану та аналіз діючих технологій захисту електронних транзакцій під час Інтернет - еквайрингу.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

1 Зробити огляд існуючих криптографічних протоколів, зокрема SSL,SET, OBI, OFX, IOTP, 3-DSecure.

2 Проаналізувати вміст криптографічних перетворювань, які використовуються в діючих технологіях захисту електронних транзакцій.

3 Порівняти технології захисту електронних платіжних систем.

4 Визначити переваги та недоліки сучасних технологій захисту електронних транзакцій.

5 Зробити висновки щодо стану технологій захисту електронних транзакцій.

Для захисту електронних транзакцій під час Інтернет-еквайрингу необхідно використовувати надійні механізми захисту електронних платіжних систем. Саме з цією метою використовуються сучасні криптографічні протоколи захисту інформації (шифрування, розподілення ключів та автентифікацію) [1].

Здійснення електронних платежів містить в собі процеси авторизації і шифрування інформації в мережі Інтернет з використанням протоколів SSL (SecureSocketsLayer) і SET (SecureElectronicTransaction). Протокол SSL припускає шифрування інформації на канальному рівні, а протокол SET– шифрування виключно фінансової інформації.

Протокол SSL– один з існуючих протоколів обміну даними, який був створений для безпечного передавання повідомлень за допомогою мережі Інтернет, він забезпечує шифрування інформації, що передається телекомунікаційними каналами. Широке розповсюдження протоколу SSL пояснюється тим, що він є складовою частиною багатьох Web-браузерів і Web-серверів. Це означає, що власник картки, що має стандартні засоби виходу в Інтернет, може здійснювати платіжні транзакції за допомогою протоколуSSL.

Недоліком протоколу SSL є відсутність автентифікації клієнта у транзакціях, що дозволяє шахраєві успішно здійснювати розрахунки лише за допомогою вкрадених реквізитів платіжної картки. Тим більше, протокол SSL не дозволяє ідентифікувати клієнта банком, який його обслуговує. Крім того, автентифікація торгового підприємства тільки за URL-адресою полегшує шахрайський доступ до різних платіжних систем, а також при використанні SSL не забезпечується конфіденційність даних про реквізити картки.

Протокол SSL є стандартом, заснованим на криптографії з відкритим ключем і передбачає можливість обміну ключами за допомогою алгоритму Діффі-Хеллмана та використання асиметричного алгоритму RSA.

Розробку протоколу SSL здійснювала компанія Netscape Communications для додання протоколу HTTPS до свого веб-браузера Netscape Navigator. Надалі, на підставі протоколу SSL 3.0 було прийнято стандарт RFC, який у подальшому отримав назвуTLS. TLS — це протокол, що був уведеним в дію на підставі протоколу SSL організацією IETT, яка створила відповідний стандарт. ПротоколTLS забезпечує можливість повторного підключення без додаткової автентифікації і узгодження ключів сеансу. Протокол може забезпечити узгодження допустимих криптографічних алгоритмів: генерування ключів (DH); шифрування (RC2, RC4, IDEA, DES, 3-DES, AES, Blowfish); цифрового підпису та автентифікації (DSS, RSA); гешування (SHA-1, MD5).

ПротоколSSL/TLSдозволяє вирішити частину проблем безпеки, зазвичай, функції протоколу обмежуються застосуванням шифрування даних, які передаються через мережу Інтернет. Крім того, за допомогою цього протоколу можна перевірити, що дані передаються на відповідний сервер. Проте, через технічні та ліцензійні особливості протоколу SSL, він вважається не дуже надійним.

Тому для комплексного рішення всіляких проблем платіжними системами Visa і MasterCardбуло створено набір протоколів, що відомі як стандарт SET (Secure Electronic Transactions) «Безпечні електронні транзакції». У цьому протоколі для захисту транзакцій при здійсненні електронних платежів використовуються дві процедури: по-перше, шифрування та по-друге, автентифікація за допомогою цифрового підпису. Протокол гарантує, що при взаємодії власника пластикової карти і продавця, інформація про рахунок кредитної карти залишатиметься конфіденційною (використовується подвійний цифровий підпис) [4–8] .

Завдяки своєї відкритості, протокол SET дозволяє розробникам створювати рішення, які можуть взаємодіяти між собою. Крім того, він базується на існуючих платіжних системах, які стали звичним фінансовим інструментом з налагодженою технологією та правовим механізмом і саме це є важливим фактором, що забезпечує просування технології SET.

В основі системи безпеки, яка використовується технологією SET, лежать криптографічні алгоритми 3-DESi RSA. Інфраструктура SET побудована відповідно до інфраструктури відкритого ключа PKI (Public Key Infrastructure,) на базі сертифікатів, що відповідають стандарту X.509, затвердженим організацією зі стандартизації (ISO).

Перевагою протоколу SET є повна конфіденційність угоди. Також перевагою даного стандарту можна відзначити посилення безпеки, включаючи можливість автентифікації всіх учасників транзакції.

Проте протокол SETпід час електронних розрахунків розпочинає свою роботуbколи користувач саме натискає клавішу оплати, але до того часу, взаємодія користувачів нет -еквайрингу регламентується протоколом IOTP (Internet Open Trading Protocol,«Відкритий торгівельний Інтернет протокол»). Протокол спроектований у такий спосіб, щоб забезпечити його придатність за будь-яких схем електронних транзакцій, в яких перерахування грошей є лише одним кроком з багатьох. Схеми платежів, що підтримує протокол IOTPвикористовують різні платіжні системи, серед якихMasterCardCredit, VisaCredit, MondexCash, VisaCash, GeldKarte, eCash, CyberCoin, Millicent, Proton. Протокол електронної комерції IOTP є найбільш складним з більш ніж чотирьох сотень протоколів, розроблених IETF [15;16].

Варто згадати стандарт OBI«Відкриті придбання в Інтернеті»,що суттєво спрощує процес купівлі через мережу Інтернет та зменшує вартість послуги. Крім того, підвищується рівень сервісу в процесі обслуговування клієнтів. Метою OBI було автоматизувати обробку транзакцій на невеликі суми, які складають приблизно 80% від обороту, що привело до економії на обробці транзакцій. Застосування OBI дозволяє істотно знизити витрати і зменшити обсяги закупівель, які здійснюються без укладання контрактів, що підвищує ефективність торгівлі і надійність угод.

Слід зазначити протокол OFX (Open Financial Exchange) "Відкритий фінансовий обмін ", який забезпечує підтримку наступних операцій через Інтернет: переказ коштів; здійснення платежів; виставляння й оплата рахунків; витяги по рахунках, виписки історії транзакцій, поточний стан рахунків і т. ім. OFX спрощує фінансовим установам з'єднання безлічі споживчих інтерфейсів, збільшуючи можливості фінансових установ в реалізації фінансових послуг в режимі реального часу. Для підтримки специфікації OFX лідери фінансового ринку — Bank of America, Chase Manhattan Bank, Citibank, First Technology Credit Union, Key Bank, Wells Fargoi Wood forest National Bankоб'єдналися в Комітет з управління відкритим обміном фінансовою інформацією в банківській сфері (Open Financial Exchange Banking Steering Committee), а брокерські компанії (Fidelity Investments, Charles Schwab і Dean Witter) сформували окреме об'єднання - Комітет з управління брокерською діяльністю (Brokerage Steering Committee).

Створення перерахованих вище стандартів сприяло спрощенню і зростанню популярності послуг онлайнового банківського обслуговування, дозволило скоротити число шахрайських транзакцій, але складність впровадження і використання технології SET стримує їх повсюдне застосування.

Отже недоліками протоколу SET є технологічна складність,велика вартість впровадження цієї технології і дорожнеча у використанні. Крім того, рівень шахрайства в мережі доки ще дозволяє користуватися доступнішими протоколами.

З метою підвищення рівня безпеки електронних платежів, корпорація VISA розробила протокол 3-DSecure і запропонувала клієнтам послугу Verified by Visa (VbV). Послуги, що ґрунтуються на підставі цього протоколу також були прийняті компаніями MasterCardпід назвою Master Card Secure Code (MCC) і JCB International як J/Secure.

Сучасний протокол 3-D Secure позбавлений недоліків протоколу SET, які заважають його впровадженню, а саме: він дешевше в реалізації, зручніший у використанні і додає ще один крок автентифікації при здійсненні електронних платежів.

При здійсненні платежу картою банку, що підтримує протокол 3-D Secure, до необхідної інформації додається додатковий запит на підтвердження дійсності карти (звичайно це одноразовий пароль підтвердження, який надсилається банком в SMS - повідомленні на відповідний мобільний телефон клієнта).Деякі банки використовують систему постійних паролів (отриманих при реєстрації) і при здійсненні кожної електронної транзакції клієнт вводить саме його. Проте такий спосіб автентифікації є менш надійним, чим одноразовий пароль підтвердження.

Доставка одноразового пароля за допомогою SMS, напевно, найпростіший спосіб надання коду для підтвердження дійсності при розрахункових операціях в мережі Інтернет. Передбачається, що, якщо клієнт ввів одноразовий пароль, у нього на руках є мобільний телефон з SIM картою, зареєстрованою в Інтернет-банку.

Проте існує безліч способів обходу такого захисту. Наразі більш популярним стає перехоплення керування смартфоном за допомогою мобільної троянської програми. Мобільний троян, що заразив пристрій, може пересилати шахраєві перехоплене SMS повідомлення з одноразовим кодом підтвердження. Далі зловмисник може використати його для продовження здійснення електронної транзакції за допомогою платіжної картки, реквізити якої він викрав заздалегідь. Проте недоліком такого зловмисного методу передачі перехопленого коду підтвердження є затримка за часом самого SMS повідомлення. Але наразі під час електронної транзакції деякі банки нехтують додатковим захистом та не визначають допустимий час затримки SMS-повідомлення. Тому для захисту від злочину необхідно використовувати допустимий час затримки SMS-повідомлення з одноразовим кодом підтвердження.

У технології захисту 3-DSecureтакож є недоліки. В звичайних транзакціях відповідальність за операції по вкрадених картах несе підприємство, на сайті якого була зроблена купівля товару чи послуги за допомогою вкраденої карти (за умови, що він не підтримує технологію 3-D Secure). У разі ж транзакцій, які захищаються за технологією 3-D Secure, відбувається так зване "Перенесення відповідальності" (англ. Liability Shift), коли відповідальність переноситься на банк-емітент, що випустив платіжну карту, або на самого клієнта.

Проте головним недоліком технології 3-D Secure є те, що для захисту конфіденційної інформації використовується криптографічний протокол SSL/TLS, який має багато вразливостей [4]. Для додаткового захисту при здійсненні електронних платежів просто додається ще один крок автентифікації.

Дослідження стану технологій захисту електронних транзакцій дає змогу визначити переваги та недоліки сучасних технологій захисту електронних транзакцій. Рівень шахрайства в мережі поки що дозволяє користуватися протоколами, які мають вразливості. Оскільки шахрайські методи здобуття інформації під час Інтернет еквайрингу нестримно розвиваються, проте виникає необхідність виявлення уразливостей сучасних протоколів захисту та подальшого дослідження, що дасть змогу їхнього удосконалення.

Усунення виявлених недоліків підвищить безпеку транзакцій під час Інтернет - еквайрингу.

Проведений аналіз стану технологій захисту електронних транзакцій показав про необхідність подальшого дослідження й удосконалення технологій захисту електронних транзакцій в платіжних системах під час Інтернет-еквайрингу.

ВИСНОВОК

В результаті проведених досліджень:

1 Зроблено аналіз та порівняння технологій захисту електронних платіжних систем SSL, SET і 3-D Secure, що дає змогу визначити їх основні переваги та недоліки.

2 Визначено переваги та недоліки сучасних технологій захисту електронних транзакцій. Перевагою технології SET є повна конфіденційність угоди, а недоліками є висока вартість впровадження і складність використання цього протоколу захисту. До переваг технології 3-D Secure можна віднести невисоку вартість реалізації і простоту використання. Проте в технології 3-D Secure є свої недоліки. Це, по-перше, використання уразливого криптографічного протоколу SSL/TLS, хоча він «підсилюється» додатковим кроком автентифікації, і по-друге – «перенесення відповідальності» на самого клієнта (чи на банк-емітент), у разі використання зловмисником вкраденої карти. Рекомендовано для захисту від злочину під час Інтернет еквайрингу визначати допустимий час затримки SMS – повідомлення з одноразовим кодом підтвердження. Проте, якщо зловмисник разом з карткою клієнта може використовувати ще й мобільний телефон клієнта, то здійсненню шахрайского платежу практично нічого не завадить.

3 Технологія SET наразі є найбільш стійкою та надійною, але через свою складність має досить високу вартість впровадження. Проте користувачам, які використовують протоколи SSL і 3-D Secure достатньо мати звичайний браузер. Тому банки не квапляться переходити на протокол SET. До того ж рівень шахрайства в мережі поки що дозволяє використовувати менш надійні протоколи. Тому SET, не зважаючи на свій високий рівень захисту, вимагає оптимізації, щоб знизити його вартість, яка поки є головним аргументом, що перешкоджає його впровадженню.

Підводячи підсумок, можна зробити висновок про необхідність подальшого вивчення й удосконалення технологій захисту електронних транзакцій в платіжних системах.

ЛІТЕРАТУРА

1 Йона Л.Г. Криптографічний захист електронного документообігу [Текст] / Л. Г. Йона,О. О. Йона, В. С. Терешко // Цифрові технології.–2013. – № 13. – С. 142–146.

2 Балакирский В.Б. Безопасность электронных платежей [Текст] / В.Б. Балакирский // Конфидент. – 1996. – №5. – С. 47–53.

3 Гайкович В.Ю. Безопасность электронных банковских систем[Текст]: учебник / В.Ю. Гайкович, А.С. Першин. – М.: Единая Европа, 1994. – 354 с.

4 Быхно А.3D-Secure: безопасные покупки через Интернет [Электронный ресурс] / Александр Быхно. – Режим доступа:\www/URL: http://credit-card.ru/articles/security/3d-secure.php

5 Фахретдинов Р. Анализ средств подтверждения банковских транзакций [Электронный ресурс] / Руслан Фахретдинов. – Режим доступа: http://www.frodex.ru/event/authentification2014

6 3-DSecure [Электронный ресурс]. – Режим доступа:http://www.bankdbo.ru/3-d-secure

7 Інтернет-ресурс http://bankir.ru/tehnologii/s/bezopasnost-i-zaschita-internet-platejei

8 Йона О. О. Специфічні чинники активізації загроз економічній безпеці господарюючих суб'єктів [Текст] / О. О. Йона // Технологічний аудит та резерви виробництва. – 2012. –№ 4/6 (8). – С. 31-32. – Режим доступу: http://journals.uran.ua/tarp/article/view/5645

9 Йона О. О. Огляд та систематизація типових моделей загроз безпеці персональних даних, які обробляються в спеціальних інформаційних системах підприємств [Текст]/ О. О. Йона // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 8(179), Ч. 1. – С. 110-117.

10 Арістова І. В. Інформаційна безпека людини як споживача телекомунікаційних послуг[Текст]: монографія/ І. В. Арістова, Д.В. Сулацький. – К.: Ред. журн. «Право України»; Х.: Право, 2013. – 184 с.

11 JunaidAhmedZubairi, AtharMahboob.Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, 2011.

12 Cyril Onwubiko, Thomas Owens. Situational Awareness in Computer Network Defense: Principles, Methods and Applications, 2012.

13 Йона Л.Г. Защита информации в электронных платёжных системах[Текст] / Л. Г. Йона, Е.О. Йона, А. А. Запороженко // Цифрові технології – 2014. – № 16. – С. 136–140.

14 Йона О. О. Дослідження стану сучасних технологій захисту електронних транзакцій / О. О. Йона // Технологический аудит и резервы производства. − 2015. − № 2/6(22). − С. 42–44.

15 FRC 2801: Internet Open Trading Protocol – IOTP . Version 1.0E. D. Burdett, April 2000, 290p.

16 Bidgoli H. Electronic Commerce, Academic Press, 2002, 487p.

REFERENCES:

1 Yona, L. G., Yona, O. O., Tereshko, V. S. (2013). Kryptohrafichnyi zakhyst elektronnoho dokumentoobihu. *Tsyfrovi tekhnolohii, 13*, 142-146.

2 Balakirskii, V. B. (1996). Bezopasnost' elektronnyh platezhei. *Konfident, 5*, 47-53.

3 Gaikovich, V. Yu., Pershin, A. S. (1994). *Bezopasnost' elektronnyh bankovskih sistem*. M.: Edinaia Evropa, 354.

4 Byhno, A. *3D-Secure: bezopasnye pokupki cherez Internet*. Available: http://credit-card.ru/articles /security/3d-secure.php

5 Fahretdinov, R. *Analizsredstvpodtverzhdeniiabankovskihtranzaktsii*. Available: http://www.frodex.ru/ event/authentification2014

6 3-DSecure.Available: http://www.bankdbo.ru/3-d-secure

7 Інтернет-ресурс http://bankir.ru/tehnologii/s/bezopasnost-i-zaschita-internet-platejei

8 Yona, O. (2012). Specific factors of activation risks security of a business entity. *Technology Audit And Production Reserves, 6(4(8))*, 31-32. Available: http://journals.uran.ua/tarp/article/view/5645

9 Yona, O. O. (2012). Ohliad ta systematyzatsiia typovykh modelei zahroz bezpetsi personalnykh danykh, yaki obrobliaiutsia v spetsialnykh informatsiinykh systemakh pidpryiemstv. *Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 8 (179), Part 1*, 110-117.

10 Aristova, I. V., Sulatskyi, D. V. (2013). *Informatsiina bezpeka liudyny yak spozhyvacha telekomunikatsiinykh posluh*. K.: Red. zhurn. «Pravo Ukrainy»; X.: Pravo, 184.

11 Junaid Ahmed Zubairi, Athar Mahboob. Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, 2011.

12 Cyril Onwubiko, Thomas Owens. Situational Awareness in Computer Network Defense: Principles, Methods and Applications, 2012.

13 Yona, L. G.,Yona, O. O., Zaporojenko, O. O., (2014). Information security in electronic payment system. Tsyfrovi tekhnolohii, 16. – S. 136-140.

14 Yona, O. O. (2015). Research state of modern electronic transactionsdefence technologies. Technology Audit And Production Reserves,2/6(22), 42-44.

15 FRC 2801: Internet Open Trading Protocol – IOTP . Version 1.0E. D. Burdett, April 2000, 290p.

16 Bidgoli H. Electronic Commerce, Academic Press, 2002, 487p.