Прокопишин Іван Анатолійович – кандидат фізико-математичних наук, доцент кафедри математичного моделювання Львівського національного університету імені Івана Франка.

Циктор Андрій Іванович – аспірант кафедри фінансів Університету банківської справи Національного банку України (м. Київ).

УДК 004.738.5:336.717.1

О. В. Клювак

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМ НА ОСНОВІ ПРОЦЕСНОГО ПІДХОДУ

Виокремлено основні активи в Інтернет-платіжних системах (ІПС) і загрози, які можуть виникати під час проведення Інтернет-трансакцій банківськими платіжними картками. Застосовано методику оцінки захищеності ІПС на основі системного підходу з метою виявлення найуразливіших активів та найбільш небезпечних загроз, а також побудовано функціональний профіль захищеності інформації для Інтернет-платіжних систем.

Ключові слова: *Інтернет-платіжна система (ІПС), Інтернет-транс акція, інформаційна безпека, процесний підхід, актив, загроза, функціональний профіль захищеності.*

Постановка проблеми. Оцінка захищеності інформаційних систем стала набувати особливої актуальності в Україні починаючи з 2005 року, коли почали з'являтися міжнародні стандарти з управління інформаційною безпекою. Варто зазначити, що Галузевий стандарт НБУ базується на процесному підході до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ організації (модель «Плануй-Виконуй-Перевіряй-Дій»). Тому доцільним є здійснювати оцінку захищеності ІПС саме за допомогою методики, яка передбачає процесний підхід до управління інформаційною безпекою та відстеження зміни загального рівня ризику з плином часу. Із розвитком електронної комерції в Україні почалося активне зростання кількості інтернет-платіжних систем із безліччю об'єктів, суб'єктів та різноманітними інформаційними потоками. Зрозуміло, що наслідком ускладнення ІПС є зростання множини чинників, що впливають на інформаційну безпеку, та поява нових процесів. А це зобов'язує суб'єктів електронної комерції до періодичного моніторингу та перегляду продуктивності та

© *О. В. Клювак, 2014*

ефективності систем управління інформаційною безпекою, застосовуючи при цьому процесний підхід.

Аналіз останніх досліджень та публікацій. Методика оцінки захищеності інтернет-платіжних систем опирається на провідні дослідження інформаційної безпеки [1; 2], українські та міжнародні стандарти управління інформаційною безпекою [3–4] та методиці оцінювання інформаційної безпеки [5].

Метою статті є виокремлення найуразливіших активів та найнебезпечніших загроз під час проведення інтернет-транзакції за допомогою системного підходу методики оцінки захищеності інформаційних систем, а також побудова функціонального профілю захищеності для Інтернет-платіжних систем відповідно до Нормативних документів у галузі технічного захисту інформації (НД ТЗІ) і Державних стандартів України (ДСТУ).

Обґрунтування отриманих наукових результатів. Для оцінювання рівня захищеності інформаційної системи, окрім виявлення найбільш небезпечних загроз, важливим є виявлення найбільш вразливих активів. Відповідно до Галузевого стандарту України Національного банку України «Інформаційні технології Методи захисту Звід правил для управління інформаційною безпекою» до активів відноситься усе, що повинно враховуватися для забезпечення ефективного управління інформаційною безпекою, включаючи інформацію в електронному та паперовому вигляді, програмне та апаратне забезпечення, персонал тощо. У нашому дослідженні акцентується увага на таких активах:

• інформації як активи, наприклад бази даних та файли даних, а також можна віднести автентифікаційні дані;

• програмних активах: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти, зокрема модуль комбінаційного хешування.

Призначенням методики, яка базується на процесному підході є оцінювання загального рівня захищеності ІПС, виявлення найбільш вразливих активів та найбільш небезпечних загроз під час проведення Інтернет-трансакцій, визначення пріоритетів в усуненні вразливостей ІПС. Процедура даної методики передбачає дев'ять етапів:

1. Первинне опитування клієнта;
2. Визначення активів;
3. Визначення важливості активів за словесною ознакою;
4. Пошук вразливостей визначених активів;
5. Визначення загроз, що походять від знайдених вразливостей;
6. Визначення ступеня небезпеки знайдених загроз за словесною шкалою;
7. Переведення важливості активів та ступеня небезпеки загроз у кількісні оцінки;

8. Підрахування оцінок ризиків;
9. Ранжирування за сумарними оцінками ризиків. Визначення найбільш вразливих активів та найбільш небезпечних загроз;
10. Ранжирування вразливостей кожного активу;
11. Складання рекомендацій щодо усунення вразливостей та оформлення звіту.

Розглянемо деякі етапи процедури цієї методики. Основними активами ІПС виступають такі: автентифікаційні дані; програмний модуль обчислень; сервер Інтернет-платіжної системи.

Наведемо рекомендовану шкалу оцінок важливості виокремлених активів в Інтернет-платіжних системах та оцінимо кількісно важливість наведених активів (*табл. 1* і *2*) [1–5].

Таблиця 1

Рекомендована шкала оцінок важливості активів в Інтернет-платіжних системах

Важливість активу	Збиток при реалізації загроз (умовна оцінка)
Критичний	5
Важливий	4
Рядовий	3
Маловажливий	2
Неважливий	1

Таблиця 2

Оцінки важливості активів в Інтернет-платіжних системах

Актив	Важливість активу	Збиток при реалізації загроз (умовна оцінка)
Автентифікаційні дані	Критичний	5
Програмний модуль обчислень	Критичний	5
Сервер інтернет-платіжної системи	Важливий	4

Побудовано на основі: [1–5]

Вразливостями визначених активів можуть бути наступні: перехоплення, модифікація, фальсифікація автентифікаційних даних, перехоплення інформації з сервера, злом сервера та програмного модуля та інші. Одна вразливість може бути джерелом декількох загроз. Так, наприклад перехоплення, модифікація, фальсифікація автентифікаційних даних можуть викликати загрозу спостереженості. В цілому, як вже зазначалося загрозами для знайдених вразливостей виступають загрози спостереженості, конфіденційності, цілісності, доступності. Рекомендовані рівні небезпеки загрози відображені у *табл. 3* та відповідно до них оцінено рівні небезпеки для 6 загроз в Інтернет-платіжних системах (*табл. 4*).

Таблиця 3

Рекомендована шкала оцінок ступеня небезпеки загроз в Інтернет-платіжних системах

Рівень небезпеки загрози	Частота (умовна оцінка)
Критичний	5
Важливий	4
Середній	3
Низький	2
Малоймовірний	1

Таблиця 4

Оцінки рівня небезпеки загроз в Інтернет-платіжних системах

Загроза	Рівень небезпеки загрози	Частота
Втрата спостереженості	Критичний	5
Втрата конфіденційності	Критичний	5
Втрата цілісності	Важливий	4
Втрата доступності	Середній	3
Хакерські дії	Критичний	5
Віруси	Середній	3

Побудовано на основі: [1–5]

Оцінка ризиків розраховується шляхом множення збитку активу на значення частоти загрози: $R = W \times n$, де R – ризик, W – збиток, n – частота.

Побудуємо приклад зведеної таблиці та зведеної діаграми ризиків на основі умовних оцінок для Інтернет-платіжної системи (*табл. 5*, *рис. 1* і *2*).

Таблиця 5

Зведена таблиця ризиків для Інтернет-платіжної системи

Загроза	Актив			
	автентифікаційні дані	програмний модуль обчислень	сервер Інтернет-платіжної системи	загалом
	оцінка ризику	оцінка ризику	оцінка ризику	оцінка ризику
Втрата спостереженості	25	25	20	70
Втрата конфіденційності	25	25	20	70
Втрата цілісності	20	20	16	56
Втрата доступності	15	15	12	42
Хакерські дії	25	25	20	70
Віруси	15	15	12	42
Загалом	**125**	**125**	**100**	**350**

Побудовано на основі: [1–5]

Сумарна оцінка ризику необхідна для періодичного оцінювання. Вона дає можливість відстежити зміни загального рівня ризику з плином часу. Зробити висновки щодо найвразливіших активів та найбільш небезпечних загроз в Інтернет-платіжних системах (вони мають найвищі сумарні оцінки) можна за допомогою *рис. 1* і *2* [1–5].

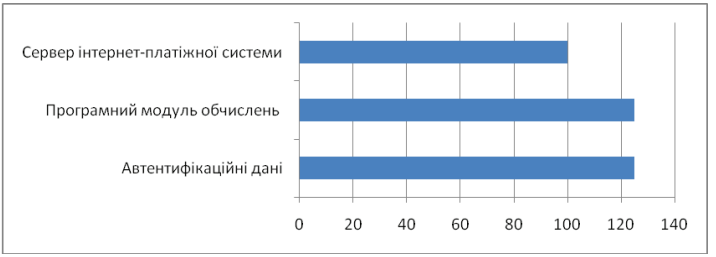

Рис. 1. **Графік сумарних оцінок за активами в Інтернет-платіжних системах**
Побудовано на основі: [1–5]

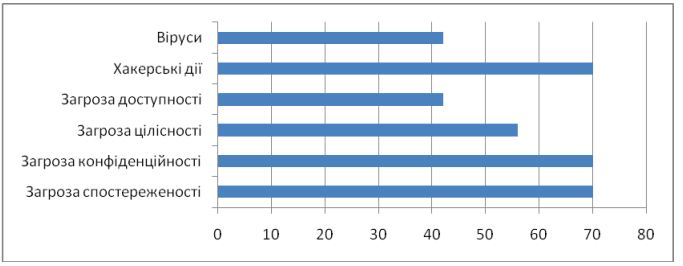

Рис. 2. **Графік сумарних оцінок за загрозами в Інтернет-платіжних системах**
Побудовано на основі: [1–5]

У процесі оцінки спроможності комп'ютерної системи забезпечувати захист інформації, котра передається під час проведення інтернет-трансакції, від несанкціонованого доступу розглядаються вимоги двох видів:

- Вимоги до функцій захисту (послуг безпеки);
- Вимоги до гарантій.

В контексті критеріїв захищеності інформації комп'ютерна система розглядається як набір функціональних послуг.

Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Рівні починаються з першого (1) і зростають до значення *n*, де *n* – унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох типів:

1. Конфіденційність. У цьому контексті можна виокремити такі послуги безпеки: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті / імпорті).
2. Цілісність. У цьому контексті можна виокремити такі послуги безпеки: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.
3. Доступність. Загрози, що відносяться до порушення можливості використання оброблювальної інформації, становлять загрози доступності. Звідси випливають критерії доступності.
4. Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. У цьому контексті можна виокремити такі послуги безпеки: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, само тестування, автентифікація при обміні, автентифікація при обміні (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Відповідно до нормативного документу системи технічного захисту інформації «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» ствердимо, що Інтернет-платіжна система належить до автоматизованих систем Класу «3», тобто ІПС є розподіленим багатомашинним багатокористувацьким комплексом, який обробляє інформацію різних ступенів обмеження доступу, тобто належить до автоматизованих систем (АС), які призначені для автоматизації банківської діяльності.

Крім того, існує необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Основні загрози для банківської інформації – це в першу чергу загрози шахрайства (підробка, відмова від авторства, відмова від одержання) і порушення технології роботи, а в другу – порушення доступності і конфіденційності. У зв'язку з цим до комплексу засобів захисту (КЗЗ) обчислювальної системи (ОС), що входять до складу банківських АС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. Крім того, вимоги істотно

залежать від того, чи здійснюється обробка в реальному часі або відкладена обробка.

Необхідно врахувати, що банківські АС, як правило, відносять до класу 3, тобто є розподіленими.

Таким чином, ІПС рекомендується використовувати обчислювальну систему, комплекс засобів захисту яких реалізують профілі 3. КЦД.х., тобто в ІПС ставляться підвищені вимоги до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Побудуємо функціональний профіль захищеності для ІПС відповідно до нормативного документа системи технічного захисту інформації «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (*рис. 3*).

3. КЦД.6 = { КД-4, КА- 3, КО-1, КК-1, КВ-3, ЦД-4, ЦА-3, ЦО-2, ЦВ-3, ДР-1, ДС-3, ДВ-2, НР-5, НИ- 3, НК-2, НО-2, НЦ-3, НТ-2, НА- 2 Г-7, , НВ-3, НП -2 }	
Позначення послуг:	
КД — довірча конфіденційність; КА — адміністративна конфіденційність; КО — повторне використання об'єктів; КК — аналіз прихованих каналів; КВ — конфіденційність при обміні; ЦД — довірча цілісність; ЦА — адміністративна цілісність; ЦО — відкат; ЦВ — цілісність при обміні; ДР — використання ресурсів; ДВ — стійкість до відмов; ДЗ — гаряча заміна; ДВ — відновлення після збоїв;	НР — реєстрація; НИ — ідентифікація і автентифікація; НК — достовірний канал; НО — розподіл обов'язків; НЦ — цілісність КЗЗ; НТ — самотестування; НВ — автентифікація при обміні; НА — автентифікація відправника; НП — автентифікація одержувача

Рис. 3. **Функціональний профіль захищеності для Інтернет-платіжних систем**
(Власна розробка на основі: [6–9])

З побудованого профілю стає зрозумілим, що такі послуги, як автентифікація при обміні, автентифікація відправника, автентифікація одержувача, а також достовірний канал, є особливо важливими при проведенні транзакцій в інтренет-платіжних системах.

Розглянемо детальніше необхідні рівні послуг критеріїв спостережності саме для Інтернет-платіжної системи (*табл. 6*).

Таблиця 6

Послуги критеріїв спостереженості профілю З.КЦД.6 для Інтернет-платіжних систем

Назва послуги критерію спостереженості профілю З.КЦД.6	Рівень даної послуги з *n* можливих	Необхідна умова	Опис рівнів послуги
Ідентифікація і автентифікація	НИ-3. Множинна ідентифікація і автентифікація (максимальний рівень)	НК-1	Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації. • Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ (Рівень 1); • Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищених механізмів двох або більше типів (Рівень 2) • КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування (Рівень 3)
Достовірний канал	НК-2. Двонаправлений достовірний канал (максимальний рівень)	немає	• Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ (рівень 1); • Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача (Рівень 2)
Ідентифікація і автентифікація при обміні	НВ-3: Автентифікація з підтвердженням (максимальний рівень)	немає	•Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації (Рівень 1); • КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується (Рівень 2); • Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною (Рівень 3)

Закінчення табл. 6

Назва послуги критерію спостережності профілю 3.КЦД.6	**Рівень даної послуги з *n* можливих**	**Необхідна умова**	**Опис рівнів послуги**
Ідентифікація і автентифікація при обміні	НВ-3: Автентифікація з підтвердженням (максимальний рівень)	немає	• Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації (Рівень 1); • КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується (Рівень 2); • Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною (Рівень 3)
Автентифікація відправника	НА-2: Автентифікація відправника з підтвердженням (максимальний рівень)	НИ-1	• Політика автентифікації відправника (одержувача) повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника (отримувача) і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (одержаний) певним користувачем (Рівень 1); • Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності (отримання) об'єкта незалежною третьою стороною (Рівень 2); • Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності (факту отримання) об'єкта незалежною третьою стороною(Рівень 2)
Автентифікація отримувача	НП-2: Автентифікація отримувача з підтвердженням (максимальний рівень)		

Побудовано на основі: [6–9]

Висновки. Таким чином, найвразливішими акивами в ІПС є: автентифікаційні дані, програмний модуль обчислень, сервер Інтернет-платіжної системи. Для них найнебезпечнішими загрозами виступають: порушення спостереженості, конфіденційності, цілісності, доступності.

Відповідно до побудованого функціонального профілю захищеності в ІПС повинні бути передбаченні максимальні рівні послуг ідентифікації та автентифікації, зокрема автентифікації отримувача і відправника з підтвердженням, та достовірного каналу. Варто зазначити, що використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною. Такою третьою стороною під час проведення інтернет-трансакції однозначно може виступати банківські установи: банк-емітент (банк покупця) і банк-еквайєр (банк продавця). Тобто для підвищення рівня безпеки проведення трансакцій необхідно застосовувати метод автентифікації, який передбачає тісну взаємодію держателя картки та його банківської установи, і метод передачі автентифікаційних даних, наприклад, на основі хешування для забезпечення послуги «достовірний канал» функціонального профілю захищеності.

Список використаних джерел

1. Домарев В. В. Безопастность информационных технологий. Системний подход / В. В. Домарев. – К. : ООО «ТИД» «ДС», 2004. – 992 с.
2. Домарев В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В. В. Домарев, Д. В. Домарев. – Донецьк : «Велстар», 2012. – 146 с.
3. Інформаційні технології Методи захисту: Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – Офіц. вид. – К. : Національний банк України, 2010. – 149 с. – (Галузевий стандарт України).
4. Information security Management systems (ISMS) [Текст]: BSI Standart 100-1, version 2.0. – Bonn : BSI, 2008. – 38 p.
5. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К. : Національний банк України, 2011.
6. Указ Президента України «Положення про технічний захист інформації в Україні» : затверджено від 27 вересня 1999 року № 1229/99. – Режим доступу : http:// zakon.rada.gov.ua.
7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99)). – [Чинний від 1999 – 04 – 28 № 22]. – К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – 16 с.
8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99). – [Чинний від 1999 – 04 – 28]. – К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – 53 с.
9. Захист інформації. Технічний захист інформації. Терміни та визначення (ДСТУ 3396.2-97). – [Чинний від 1998 – 01 – 01]. – К. : Державна служба спеціального зв'язку та захисту інформації, 1998. – 6 с. – (Державний Стандарт України).

Клювак О. В.

Методика оценки защищенности Интернет-платежных систем на основе системного подхода

Выделены основные активы в Интернет-платежных системах (ИПС) и угрозы, которые могут возникать во время проведения интернет-траназкций банковскими платежными карточками. Использована методика оценки защищенно-

сти ИПС на основе системного подхода с целью выявления уязвимых активов и наиболее опасных угроз, а также построено функциональный профиль защищенности для Интернет-платежных систем.
Ключевые слова: *Интернет-платежная система (ИПС), Интернет-транзакция, процессный подход, актив, угроза, функциональный профиль защищенности*

Klyuvak O.

Method of the trusted internet-payment systems evaluation based on the process approach.

It is determined main assets in internet-payment systems (IPS) and threats, which can arise during the internet-transaction realization. It is applied the method of the trusted internet-payment systems evaluation based on the process approach to identify the most vulnerable assets and most dangerous threats, and built the functional profile of safety functional profile of safety for internet-payment systems.
Keywords: Internet *payment system (IPS), Internet transaction, process approach, assets, threats, functional profile of safety*

Клювак Оксана Володимирівна – заступник начальника наукового відділу Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ).

УДК 336.741.242

Х. Ю. Іванюк

СИСТЕМА КОМПЕТЕНТНІСНОЇ ДІАГНОСТИКИ І ПІДВИЩЕННЯ РІВНЯ ЗНАНЬ АУДИТОРІВ

У роботі аудиторів дуже важливим є узгодження їхніх знань, умінь і навичок з вимогами, що відповідають їхній посаді. Для досягнення необхідного рівня знань аудиторів запропоновано використовувати автоматизовану систему, спрямовану на подолання інтервалу між необхідними і наявними компетенціями, а також на зменшення цього інтервалу в стислі терміни. Для вирішення поставлених завдань спроектовано систему автоматизованого оцінювання та підвищення знань аудиторів. Ця система дозволяє користувачеві самостійно оцінювати власні знання та, залежно від результатів здійснювати самостійне навчання для підвищення знань, а також здійснювати контроль знань для групи осіб. Головними перевагами системи є модульність, гнучкість і спеціалізований контроль якості навчання. Надалі планується розвиток системи у змістовному та інтелектуальному плані.
© Х. Ю. Іванюк, 2014