



*Нестеренко Олександр Васильович, доцент кафедри системного аналізу та інформаційних технологій Національної академії управління, к.т.н., доцент, академік Міжнародної академії інформатики*

## БЕЗПЕКА ЕКОНОМІКИ ЗНАНЬ

Людство впевнено просувається до інформаційного суспільства, економіка і бізнес стають електронними (цифровими) і здійснюються в глобальному середовищі (в Інтернеті). Розвиток електронної комерції не лише збільшив об'єм інформації, що обробляється і зберігається, але й підвищив її значущість та критичність. Останнім часом на порядку денному постає питання видобування з накопиченої інформації нового знання та використання його для підтримки прийняття рішень та розвитку економіки (Data Mining, Knowledge Mining, BigData). Інтелектуалізація різних систем, що набуває розмаху, підсилює «знаннєвий» рівень інформації.

Водночас необхідно звернути увагу на той факт, що кожний крок в розвитку інформаційних технологій приховує в собі потенційні загрози. Небезпеки пов'язані з атаками кіберзлочинців (шахраїв), витоком інформації, а також комерційним шпигунством. Причинами цих загроз є численні точки доступу, зв'язки за Інтернет-протоколами, розвиток і використання бездротових пристроїв (радіодоступ), недосконалі правила додержання вимог безпеки, недостатня свідомість персоналу [1].

Поява нових, більш прихованих загроз, у зв'язку з перспективами сплеску мобільного Інтернету та Інтернету речей за технологіями 4G та 5G вимагає своєчасного підвищення ефективності систем безпеки на багатьох рівнях - інакше для світової віртуальної економіки настануть не найкращі часи.

Виходячи з математично доказаного постулату неможливості абсолютного захисту фундаментальним поняттям інформаційної та кібербезпеки виступає довіра. Це пов'язано з людиною як одним з суб'єктів безпеки. На перший план виходить проблема створення простору довіри для безпечного ведення бізнесу в електронному виді. У фізичному (реальному) світі людину або супроводжуючи документи можна побачити. У цифровому (віртуальному) світі усі спілкуються



## Formation of knowledge economy as the basis for information society



один з одним через комп'ютер, тобто питання розпізнавання особи, організації, документів, довіри до них стає визначальним.

Ще 1985 р. у «Критеріях оцінки захищеності комп'ютерних систем» (США), була проголошена ініціатива захищених комп'ютерних систем, що зводиться до висловлювання: «Захищена комп'ютерна система дозволяє людині або організації сказати: «Я можу довіряти цьому продукту або сервісу. Він надійний, захищений та моя приватна (комерційна) інформація поважається» [4].

Які ж технології необхідно використовувати для забезпечення довіри? Сучасна концепція кібербезпеки включає низку методів і засобів, серед яких необхідно виділити такі як шифрування, довірена ідентифікація, вільне/відкрите програмне забезпечення та хмарні технології.

Засоби шифрування вже давно вийшли з секретних кабінетів і широко використовуються в забезпеченні конфіденційності комерційної інформації завдяки відкритості стандартів та алгоритмів, а також зниженню дозвільних бар'єрів. Реалії небезпечності інформаційного середовища доводять, що майбутнє за суцільним шифруванням інформації на усіх щаблях її опрацювання.

Згідно з Національною стратегією довіреної ідентифікації в кіберпросторі, розробленою в США, довірене Інтернет-середовище є таким, в якому окремі особи, організації, служби і пристрої можуть довіряти один одному, тому що авторитетні джерела встановили достовірність їх цифрових посвідчень. Цифрова ідентичність - це набір атрибутів об'єкту (людини або організації) в певній області.

Для роботи з масовими користувачами широко використовується автентифікація на основі цифрових сертифікатів стандарту X.509 і інфраструктури публічних ключів (PKI) електронного цифрового підпису. Додатковий атрибутний сертифікат X.509 зв'язує атрибути прав доступу з власником сертифікату і призначений для використання в Інтернет - додатках. В атрибутні сертифікати включають додаткову інформацію про суб'єкта, який ставить цифровий підпис. Ця інформація дозволяє упевнитися, що суб'єкт має право підписувати дані. Унікальність значення ідентифікатору об'єкту (IO), що відрізняється від інших подібних значень і який пов'язується з інформаційним об'єктом, забезпечується



## Формування економіки знань як базису інформаційного суспільства



упорядкованим списком первинних цілочисельних значень від кореня (Root) міжнародного дерева ІО до вершини, який однозначно ідентифікує цю вершину. Рекомендацією ІТУ-Т Rec.X.660 | ISO/ ІЕС 9834-1 визначено міжнародне дерево ІО, яке підтримує дерево ідентифікаторів у кодах стандарту ASN.1 і міжнародний опис ідентифікаторів, а також зв'язок між ними [2]. Українське дерево ідентифікаторів об'єктів (OID-TREE UA) починається з головного вузла, значення якому привласнене відповідно до міжнародних рекомендацій, і має дві гілки - 1.2.804 та 2.16.804:

{iso(1) member-body(2) ua (804)};

{joint-iso-itu-t (2) country (16) ua (804)}.

На часі нова робота, що проводиться за підтримкою Глобальної ініціативи МСЕ-Т по стандартах управління визначенням ідентичності, що стосується загальної довіри і функціональної сумісності. Використання Рекомендацій X.1250 «Базові можливості для покращеної довіри і функціональної сумісності при глобальному управлінні визначенням ідентичності (IdM)» приведе до розробки структури для завтрашніх інфраструктур і послуг мереж на базі ІР.

Основні переваги вільного/відкритого програмного забезпечення (ВПЗ), що беруться до уваги урядами багатьох країн, у тому числі і європейських, при його впровадженні пов'язані не лише з економічними питаннями, а передусім з забезпеченням безпеки і впевненості у незалежності від іноземного постачальника [3].

Переваги хмарних обчислень, які набувають стрімкого поширення, включають не лише гнучке і динамічне надання ресурсів і спрощене автоматизоване адміністрування ІТ-інфраструктури, а й забезпечення довіри [4]. У проектах Рекомендацій МСЕ-Т X.ccsec, X.srfcts і X.sfcse міститься набір рекомендацій щодо послуг в сфері безпеки, які стосуються аналізу, архітектури і структури безпеки хмарних обчислень, їх міжрівневої безпеки, а також конкретних питань безпеки мережевих послуг.

1. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко – К.: Наук. думка, 2009. – 352 с.



2. Юдін О. К. Світовий простір ідентифікаторів об'єктів: аналіз, перспективи розвитку, місце українського сегменту / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. – 2014. - № 3 (23). – С. 295-302.
3. Будько М.М. Вільне програмне забезпечення: український вибір / М.М. Будько, О.В. Нестеренко, І.Є. Нетесін. – К.: Альтерпрес, 2011. – 400 с.
4. Rhoton J. Cloud Computing Explained: Implementation Handbook for Enterprises / John Rhoton. – Recursive Press; 2nd ed., 2009. – 472 pages.

### **СЕКЦІЯ 1. ЕКОНОМІЧНІ ЗАСАДИ ТА ІНФОРМАЦІЙНА ОСНОВА ФУНКЦІОНУВАННЯ ЕКОНОМІКИ ЗНАНЬ**

*Алексеєнко Людмила Михайлівна, д.е.н., професор, завідувач кафедри обліку та фінансів, Івано-Франківський навчально-науковий інститут менеджменту Тернопільського національного економічного університету*

*Алексеєнко Максим Дмитрович, д.е.н., професор, професор кафедри банківської справи, Київський національний економічний університет імені Вадима Гетьмана*

*Карпа Ірина Степанівна, аспірантка кафедри фінансів суб'єктів господарювання і страхування, Тернопільський національний економічний університет*

#### **ІННОВАЦІЙНІ ФІНАНСОВІ ТЕХНОЛОГІЇ В УМОВАХ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА**

Розвиток інноваційних фінансових технологій став можливим завдяки науково-технічному прогресу, зростанню ролі знань і інформації в сучасному суспільстві. Це зумовило руйнування закономірностей, що були визнані економічною наукою, щодо розвитку різних фінансово-економічних систем і їх елементів. Г. Джеймс відзначає, що термін «глобалізація» з'явився недавно, але інтернаціоналізація ринків, людей, ідей і культур зовсім не нова [1].

Теоретичний і емпіричний етапи наукового дослідження інституціональної трансформації інноваційних фінансових технологій фінансового ринку забезпечують сукупність дослідних заходів та методів [2]. На емпіричному рівні дослідний об'єкт відображається, як правило, здебільшого з позицій зовнішніх зв'язків і відносин. Відповідно наукове знання і процес його здобуття