УДК 004.056.53

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Вовкодав О.В.[1)], Вовкодав В.В.[2)]
Тернопільський національний економічний університет
1) к.т.н., ст. викладач, 2)магістрант

I. Постановка проблеми

Зростання обсягів продажу товарів і послуг через мережу Інтернет – один з найбільш помітних трендів розвитку сучасного бізнесу. Все більше компаній розглядає всесвітню павутину як інструмент для збільшення прибутку і знаходження нових клієнтів. Саме це стало причиною того, що питання електронної комерції стає дедалі актуальнішим, адже в сучасних реаліях її популярність стрімко зростає. Важливим питанням в формуванні теоретичних основ цього поняття стають форми електронної комерції та її місце в системі цифрової економіки.

II. Мета роботи

Метою дослідження є аналіз існуючих систем забезпечення інформаційної безпеки у сфері електронної комерції, що формує собою досить серйозну і непросту проблему. Системи електронної комерції на Вітчизняному ринку досить молоді, значна частина організаційно-правових відносин ще тільки формуються і закріплюються, втручання в комп'ютерні системи набагато складніше виявити і розкрити, що пояснюється все вищою і вищою кваліфікацією охочих отримати доступ до закритої інформації з будь-якої точки планети із використанням систем віддаленого доступу та глобальної мережі Інтернет.

III. Методи забезпечення безпеки в системах електронної комерції

Розвиток інформаційних і телекомунікаційних технологій призвів до надзвичайної залежності сучасного суспільства від електронної обробки, зберігання, доступу і передачі інформації та управління різними процесами за допомогою комп'ютерної техніки [1]. З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють наступні напрямки захисту інформації:1) правовий захист – це спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;2) організаційний захист – це регламентація діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнюють неправомірне оволодіння конфіденційною інформацією і про явище внутрішніх і зовнішніх загроз; 3) інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації. Для реалізації захисту інформації створюється система безпеки.

Досліджуючи електронну комерцію для формування систем інформаційної безпеки, перш за все потрібно звертати увагу на ті з них, що досягли певного рівня інформаційного розвитку, адже платформою для розвитку електронної комерції є достатній рівень інформатизації суспільства та розвинена телекомунікаційна інфраструктура. Величина структурної одиниці, що визначена як «ціль» для втручання, формує собою певний перелік категорій загроз.

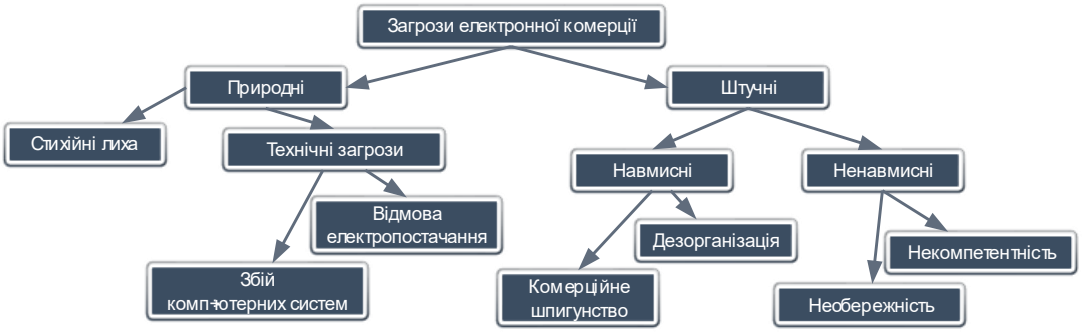

Рисунок 1 – Класифікація загроз електронної комерції

Основними вимогами, що висуваються до системи інформаційної безпеки у сфері електронної комерції, є: законність, співпраця і взаємодія, відповідальність, комплексність захисту, своєчасність реагування на погрози і зведення їх до мінімуму. Важливо в системі інформаційної безпеки електронної комерції визначити, класифікувати і ранжувати загрози. Оскільки відносини у сфері

електронної комерції відзначаються великою різноманітністю, включають різних учасників, мають різні характеристики і потребу різного ступеня захищеності, тому й загрози їхній безпеці різноманітні.

Забезпечення інформаційної безпеки частково можливо досягти використовуючи, при побудові нового суб'єкта електронної комерції, перевірених моделей функціонування електронного бізнесу. В електронному бізнесі прийнято виділяти наступні моделі взаємодії учасників ринку (Рис.2.):B2C (Business-to-Consumer) - фірма-споживач; B2B (Business-to-Business) – «фірма-фірма»; C2B (Consumer-to-Business) – «споживач-форма»; C2C (P2P ─ Peer-to-Peer, «рівний-рівний») «споживач-споживач»; B2G або B2A (Business-to-Governmpnt, Business-to-Administration) ─ «фірма-держава»; G2B або A2B (Government-to-Business) ─ «держава-фірма»; G2C або A2C (Government-to-Consumer або Administration-to-Consumer) ─ «держава-споживач»; C2G або C2A (Consumer-to-Government) ─ «споживач-держава»; G2G або A2A (Government-to-Government) ─ «держава-держава»; E2E (Exchange-to-Exchange) ─ «біржа-біржа»; інтернет банкінг; інтернет-трейдинг; інтернет-послуги. [2].

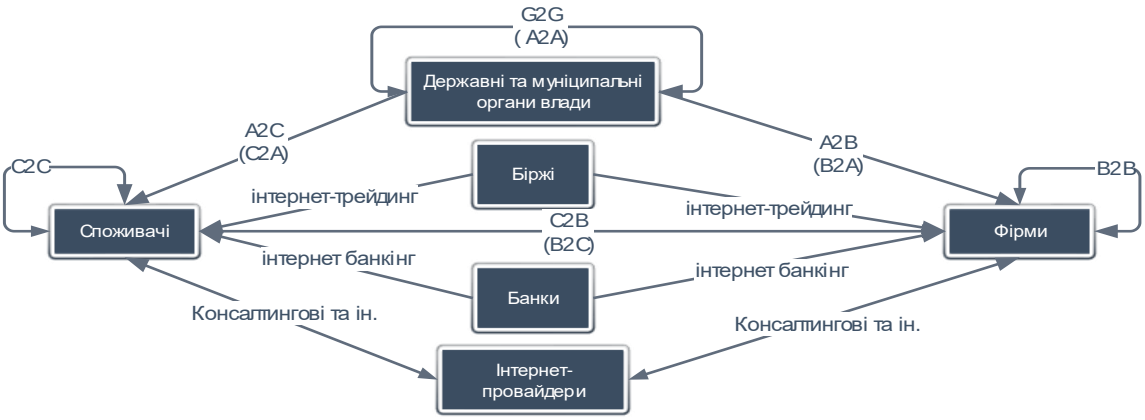

Рисунок 2 – Моделі електронного бізнесу

Основні методи визначення актуальності загроз раніше, безпосередньо, залежала від початково прийнятих засобів захисту інформації, то на сьогоднішній день, вихідні засоби захисту впливають на потенціал порушника який потім вже впливає на актуальність загрози. Інформаційна модель систем аналізу рівня величини загроз представлена у вигляді інформаційно-організаційної схеми на рис. 3.

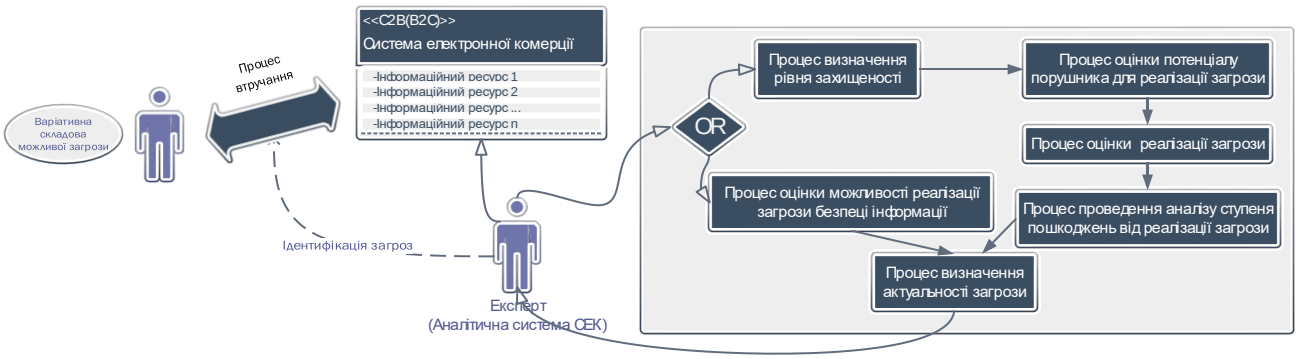

Рисунок 3 – Загальна модель процесу визначення загроз інформаційній безпеці

Висновок

У роботі досліджено задачу ефективного підвищення рівня інформаційної безпеки систем електронної комерції. Представлений короткий аналіз існуючих інформаційних моделей для побудови електронного бізнесу. Провівши аналіз сучасних систем електронної комерції, а також актуального питання загроз інформації в існуючих системах, запропоновано побудову інформаційно-аналітичної моделі визначення рівня впливу загроз інформації, що в свою чергу дозволить побудувати інформаційну структуру аналітичного забезпечення для проведення аналізу вразливостей та оцінки захищеності інформаційної безпеки в системах електронної комерції.

Список використаних джерел

1. Вовкодав О. В. Інформаційна безпека підприємства / О. В. Вовкодав, Р. Ю. Кіх. // Математичні методи, моделі та інформаційні технології в економіці: Матеріали V Міжнародної науково-методичної конференції. Чернівці «Друк Арт». – 2017. – С. 51–52.
2. Системи електронної контент-комерції: Монографія / А.Ю. Берко, В.А. Висоцька, В.В. Пасічник. – Львів: Видавництво Національного університету «Львівська політехніка», 2009. – 612 с.