послідовне підвищення рівнів їх розвитку. Це, разом з іншим, дозволило б сервісним підприємствам гнучко реагувати на нові умови господарювання.

Література

1. Дич Л.З. Биллинговые системы в телекоммуникациях / Л.З. Дич. – М.: Радио и связь. – 2003 г. – 229 с.
2. Методи алгоритмізації білінгових завдань у корпоративних комп'ютерних системах: Автореф. дис. канд. техн. наук: 05.13.06 / Д. М. Бугас; Нац. аерокосм. ун-т ім. М.Є. Жуковського "Харк. авіац. ін-т". – 2005. – 19 с.
3. Муссель К.М. Предоставление и биллинг услуг связи. Системная интеграция / К.М. Муссель. – М.: Эко-Трендз, 2003. – 320 с.
4. Системні моделі та методи прогресивної інформаційної технології управління діяльністю підприємств зв'язку: Автореф. дис. канд. техн. наук: 05.13.06 / Р.О. Гузій; Черкаський держ. технологічний ун-т. – Черкаси, 2007. – 20 с.
5. Ченцова И.И. Интеграция биллинга с информационными системами предприятия / И.И. Ченцова // Мобильные системы. – 2002. – №5. – С. 67-69.

УДК 004:339.1

Кирилюк М.С.

Врахування ризиків у процесі взаємодії електронних магазинів та користувачів

Розглядаються ризики, які виникають у відвідувачів електронних магазинів, а також пропонуються можливі заходи безпеки при онлайн-купівлі товарів. Описуються ризики, яким підлягають самі Інтернет-магазини, та наводяться пропозиції щодо підвищення безпеки веб-ресурсу, розміщеного в мережі Інтернет.

Ключові слова: *ризики, електронний магазин, відвідувач, інформаційний ризик, комерційний ризик, технічний ризик, безпека.*

Describing the risks arising at visitors of electronic shops are considered, and also possible security measures are

offered at online purchase of the goods. Risks to which Internet shops are exposed are described and offers on improvement of safety of a web resource which Internet is in a network are resulted.

Keywords: *risks, online shop, the visitor, information risk, commercial risk, technical risk, safety.*

Актуальність. Розвиток та розширення сфери застосування сучасних засобів інформаційних технологій в електронній комерції відбувається без урахування ризиків, які виникають у процесі взаємодії електронних магазинів та користувачів. Окрім цього, необхідно звернути увагу на підвищення ефективності електронної комерції, на яку вливає зручність користування сайтом, можливість швидкої та надійної оплати, якість обслуговування тощо. Сьогодні застосування електронної комерції не обмежується створенням сайту або електронного каталогу з можливістю замовлення товару, увага приділяється й впровадженню сучасних веб-технологій та накопиченню досвіду для глибинної перебудови способів ведення ділових операцій за допомогою веб та супутніх мережевих комп'ютерних технологій.

Аналіз останніх досліджень і публікацій. Зараз в літературі активно обговорюються проблеми безпеки й захисту комерційної інформації в Інтернеті, ймовірні загрози безпеці інформації в мережі. Особлива увага приділяється проблемі передачі закритої інформації (номерів кредитних карток, сум платежів, даних про клієнтів тощо) через відкриту мережну систему, оскільки вона піддається різним видам загроз. Стрімкий процес інформатизації суспільства супроводжується посиленням загроз втручання в роботу інформаційних систем у формі несанкціонованого допуску до інформації. Через це

підвищується актуальність постійного вдосконалення систем захисту інформації на основі використання комплексного підходу, який об'єднує законодавчі, організаційні та програмно-технічні заходи [1, 2].

В інформаційному суспільстві розв'язання проблем ризиків та інформаційної безпеки електронної комерції є найбільш важливою складовою забезпечення економічної безпеки електронного бізнесу. Надійність функціонування електронного бізнесу сьогодні може безпосередньо впливати на національну безпеку розвинутих інформаційних співтовариств. Цей вплив надалі буде тільки зростати [3].

Важливу роль відіграє сектор Business to Consumer (B2C), що пов'язаний з наданням послуг або продукції кінцевому споживачеві. Основний тип даних систем – це електронний магазин – автоматизована система електронної торгівлі в мережі Інтернет. Система електронної торгівлі є характерним прикладом розподіленої обчислювальної системи. У ній кілька клієнтів працюють з одним сервером, рідше з декількома серверами. Таким чином, електронному магазину загрожують всі внутрішні й віддалені атаки, притаманні будь-якій розподіленій комп'ютерній системі, яка взаємодіє за допомогою передачі даних відкритими мережами. Таким чином, обидва учасники цього бізнес-процесу – споживач та WWW-магазин виявляються уразливими та незахищеними перед можливими ризиками та загрозами [4].

Невирішеними проблемами є види ризиків в електронному бізнесі для WWW-магазинів та відвідувачів веб-сайтів.

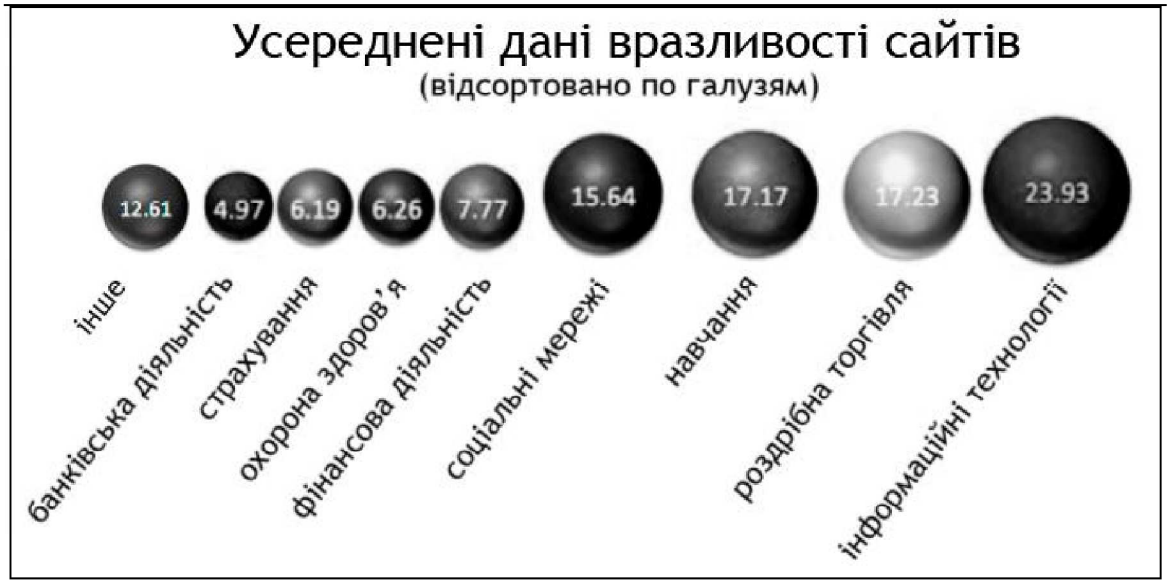
Мета статті. Провести аналіз ризиків, пов'язаних з електронними магазинами, окремо визначити ризики як

для покупців, так і для онлайн-магазинів. Провести аналіз та дослідження питань безпеки в процесі взаємодії WWW-магазинів і споживачів.

Постановка проблеми. Електронна комерція – це бізнес в мережі Інтернет, причому з кожним роком кількість онлайн-магазинів постійно зростає. Власники онлайн-бізнесу, які перебувають на ринку достатньо довго, стикаються не тільки з проблемами звичайних магазинів, такими як: наявність попиту на товар чи послугу, задоволеність клієнта, ефективна реклама, але також і з ризиками, що проявляються в мережі Інтернет.

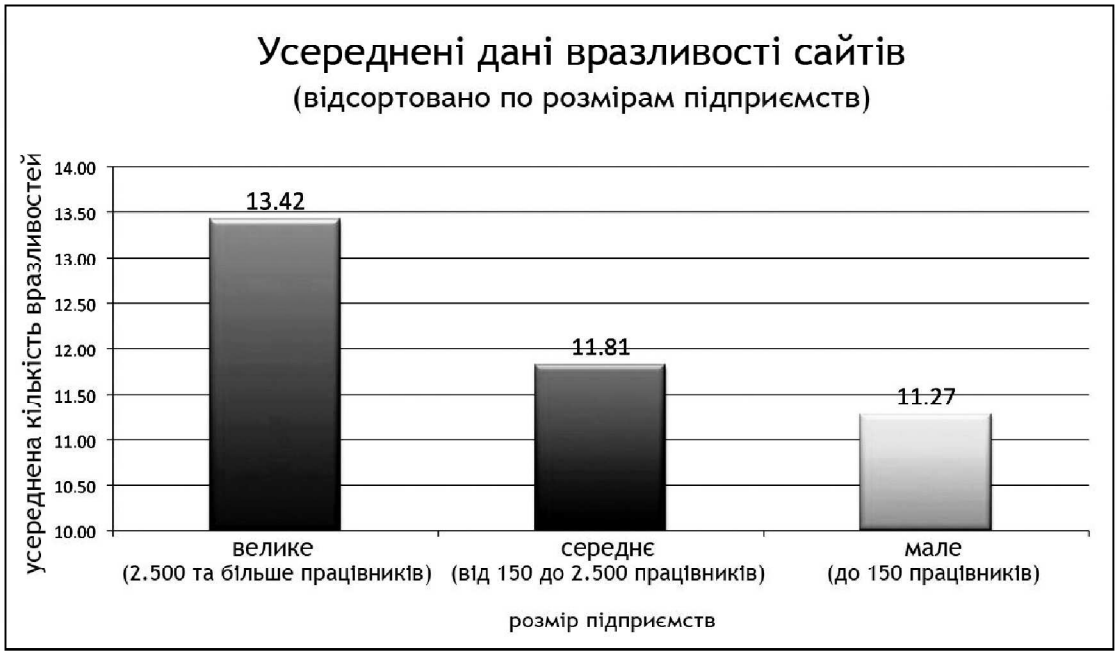
Викладення основного матеріалу. Ризики супроводжують розробку кожного веб-ресурсу, але для одних галузей їх більше, ніж для інших. Так, на рис.1 показані усереднені дані щодо серйозних загроз для сайтів, що відсортовані за галузями. Як видно з рисунка, найбільш уразливі та цікаві для зловмисників галузі – це інформаційні технології та соціальні мережі. На другому місці стоїть роздрібна торгівля й навчання. Безпека фінансової діяльності, страхування, охорони здоров'я та банківської діяльності вимагає впровадження механізмів захисту в існуючі інформаційні системи з можливістю гнучкого управління безпекою залежно від висунутих вимог, допустимого ризику та оптимальних витрат ресурсів.

Рис.2 показує кількість загроз для підприємств різних розмірів. Найбільший удар припадає на великі організації, це пов'язано з прибутковістю підприємства та його розмірами. Чим більше компанія, тим більше в ній можна знайти лазівок для злому, чим вище прибутковість, тим більш дорогу інформацію можна при цьому отримати.



Джерело [www.slideshare.net/jeremiahgrossman/website-security-statistics-report-2010-industry-bechmarks]

Рис. 1. Усереднені дані щодо вразливості сайтів залежно від галузі.



Джерело [www.slideshare.net/jeremiahgrossman/website-security-statistics-report-2010-industry-bechmarks]

Рис. 2. Усереднені дані вразливості сайтів в залежності від розмірів підприємтсва.

Нехтування ризиками в онлайн-комерції може коштувати WWW-магазину фінансових збитків, втрати довіри клієнтів та позитивного іміджу бренда.

Знизити рівень ризиків при створенні Інтернет-магазину можна при розумному підході, поетапному виконанні та плануванні всіх заходів, а також завдяки аналізу й розрахунку прибутку від онлайн-магазину. Але ризики можуть з'являтися не тільки для електронних магазинів взагалі, але й для відвідувачів та покупців WWW-магазину.

Ризиками для споживачів електронних магазинів є:

- небезпека втрати введених даних (номер кредитної карти, ім'я, адреси можуть бути перехоплені й використані для шахрайської діяльності);
- фальсифіковані продукти (продукти, які існують тільки на сторінці WWW-магазину, в реальності їх немає);
- фіктивні фірми;
- продаж товарів низької якості [5].

Безпеку споживача при онлайн-купівлях можна підвищити при:

- використанні безпечного браузера;
- встановленні та своєчасному оновленні антивірусного захисту;
- перевірці клавіатури на підключення до неї записуючих пристроїв для збору інформації при кожному натисканні кнопок, включаючи паролі;
- перевірці наявності невпізнаного програмного забезпечення на комп'ютері, деякі програми здатні записувати всі натискання на клавіатурі;
- регулярній зміні паролів;
- шифруванні інформації (процес перетворення інформації, щоб зробити її незрозумілою для всіх, окрім отримувача, лежить в основі цілісності даних і

конфіденційності, необхідних для електронної комерції);

- аутентифікації (застосовується для перевірки права доступу користувача до певних даних) [6].

Ризики можна розділити на 3 види: інформаційні ризики, технологічні ризики та бізнес-ризики. Інформаційні ризики пов'язані з інформацією, що публікується та веденням електронної комерції. До **інформаційних ризиків** належать:

- неякісний вміст веб-сторінки (наявність не унікального контенту, дублювання матеріалів, орфографічні помилки та ін.);
- порушення авторських прав (незаконне відтворення та розповсюдження матеріалів);
- злодійство, поширення та пошкодження інформації після несанкціонованого доступу до веб-ресурсу (незаконне стирання, руйнування, псування або приховування даних без права на це);
- витік інформації у зв'язку з переходом працівників до конкурентів (витік інформації, що часто супроводжується втратою клієнтів та важливих фахівців).

Технологічні ризики містять в собі ризики, пов'язані з обладнанням, програмним забезпеченням та базами даних, телекомунікаційними засобами. До цих ризиків також належать наслідки від неправильного використання технологій та/або використання невідповідних технологій, необхідних для якісного ведення онлайн-бізнесу.

Технологічні ризики:

- помилки, допущені в розробці програмного забезпечення (помилки в програмі або системі, яка видає несподіваний або неправильний результат);
- несанкціонований доступ до веб-сайту (протиправні дії, в результаті яких, зловмисник отримує доступ до закритої для сторонніх осіб інформації);

- зараження веб-сайту комп'ютерними вірусами (викликають катастрофічне падіння відвідуваності сайту, викликане вірусною позначкою, яка відображається в результатах пошуку Google та Індекс; віруси розмножуються самі й розпов-сюджують інші віруси, заражаючи інші сайти; прописують на сайті код, що дозволяє закачувати на веб-ресурс будь-які файли та керувати базою даних сайту; перехоплюють фінансову інформацію тощо);
- злам електронного магазину для продажу посилань та поширення рекламних матеріалів без дозволу власника WWW-магазину (переадресація відвідувачів з сайту на інший ресурс, нав'язливий банер, клоакінг, викрадення паролів доступу, паролів від e-mail, ICQ, Skype та інше);
- збій в роботі сервера (робота сервера призупинена або сервер працює з помилками);
- недостатня пропускна здатність сервера для обробки трафіку (сервер не надає достатню кількість даних);
- відключення послуг Інтернету провайдером при збоях на їхньому боці (провайдер призупиняє послуги без попередження зі своєї вини, як результат – сайт не працює);
- неправильна інтеграція системи електронної комерції з внутрішніми базами даних (помилки в коді програмування при інтеграції з внутрішніми базами даних);
- неправильна інтеграція системи електронної комерції з внутрішніми робочими процесами (помилки при інтеграції розрізнених бізнес-процесів, корпоративних додатків, ланцюжків постачань, сховищ даних та застарілих систем);
- неякісний програмний код та помилки користувачів (помилки в програмному коді, інтерфейсі та рівні

зручності веб-ресурсу для використання у заявлених цілях).

Комерційні ризики містять в собі ризики, які стосуються відносин з постачальниками, управлінськими аспектами бізнесу, персоналом, а також ризики, пов'язані з продуктами та послугами, які розповсюджується через Інтернет.

Комерційні ризики:

- фізичні загрози (будь-які загрози для персональних даних, які можуть дозволити стороннім людям отримати фізичний доступ до комп'ютера, а також загрози крадіжки, знищення комп'ютера, стихійних лих, пожеж та ін.);
- людський фактор (помилки співробітників);
- нанесення шкоди корпоративному іміджу бізнесу [7] (дії, що здійснюються винятково з наміром заподіяти шкоду веб-сайту, а також зловживання правами, нанесення збитку діловій репутації компанії);
- невірне позиціонування (невідповідність веб-сайту механізмам найвідоміших пошукових систем, через що виникає проблема просування сайту);
- ризики, пов'язані з оплатою онлайн в електронних магазинах (наявність обману та шахрайства при розрахунку електронними грошима зі злочинним веб-магазином);
- ризики, пов'язані з постачальниками, надання їм доступу до даних, поширення стратегії й тактики маркетингу (неправомірне поширення комерційної таємниці компанії та іншої важливої інформації);
- ризики, пов'язані з клієнтами, надання їм доступу до даних, поширення стратегії й тактики маркетингу (зловживання наданою інформацію та неправомірне її поширення);

- високі витрати на доставку (ціна доставки занадто висока, в результаті чого процес продажу товарів стає нерентабельним);
- незручна політика повернення товару або відсутність такої (за статтею 707 Цивільного кодексу України веб-покупець має право протягом чотирнадцяти днів з моменту передання йому товару неналежної якості обміняти його);
- незахищеність доменного імені (ризики пов'язані із захистом доменного імені та веб-проектів від рейдерських захоплень і блокувань роботи інтернет-магазину);
- недостатня інтеграція електронної комерції з каналами постачання товарів (основною причиною недостатньої ефективності або рівня розвитку електронних закупівель є розрив між традиційною та електронною логістикою на підприємстві) [8];
- несанкціоновані дії конкурентів або незадоволених покупців (за Законом України "Про захист від недобросовісної конкуренції") [9].

Безпеку сайта можна підвищити при використанні наступних заходів:

- резервне копіювання важливої інформації;
- ефективна кадрова політика, яка дозволяє залучати до роботи тільки сумлінних людей та стимулювати старанність персоналу (найбільш небезпечні спроби злому виходять із-середини компанії);
- використання програмного забезпечення з можливостями захисту даних та своєчасне його оновлення;
- навчання персоналу ідентифікації цілей та розпізнавання слабких місць системи;
- аудит та ведення журналів з метою виявлення успішних та невдалих спроб злому.

Бізнес у мережі Інтернет пов'язаний з ризиками, що

виникають внаслідок конкуренції, злодійства, нестійкості суспільних уподобань, стихійних лих та інше, необхідно не тільки їх виділяти, але й знати, які антиризикові заходи краще всього застосовувати [10].

Висновки

Ризики можна розділити на дві основні категорії:

- ризики, які є небезпечними для користувачів електронних магазинів (вони повинні бути впевнені, що веб-сайт є справжнім, що інформація, яку вони відправляють через веб-браузер, залишається приватною та конфіденційною);
- ризики, які є небезпечними для онлайн-магазинів.

Для WWW-магазинів ризики можна умовно розділити на три групи: інформаційні, технічні та комерційні. Інформаційні ризики пов'язані зі створенням, передачею, зберіганням та використанням інформацію за допомогою електронних носіїв або інших засобів зв'язку. Технічні ризики пов'язані зі збоями в роботі апаратури (маршрутизатор, сервер віддаленого доступу), програмного забезпечення (стандартні браузери, поштові та інші прикладні програми), а також із неполадками каналів зв'язку клієнта й сервера. Комерційні ризики – це ризики, пов'язані з можливим зниженням або втратою доходів, пов'язані з прийняттям рішень або діями в умовах невизначеності, відсутності достовірної інформації про стан ринку. Остаточно позбутися усіх ризиків неможливо, особливо враховуючи те, що іноді вартість забезпечення закритості інформації перевищує її цінність, тому для ефективного ведення онлайн-бізнесу необхідно приймати доцільні антиризикові заходи.

Важливе значення для електронного бізнесу має оцінка ефективності вкладення коштів у веб-проекти мережі Інтернет, а саме у розрахунок рентабельності

створення та просування електронного магазину. Так розробка успішних інтернет-проектів, які розраховані на довгострокову роботу, залежать не лише від якісно виконаної програмної частини, але й від ефективних методів розрахунку вкладеного початкового капіталу, які допоможуть розрахувати, наскільки окупиться WWW-магазин, до його виходу в онлайн-мережу.

Література

1. Пономаренко Л.А. Електронна комерція. // Пономаренко Л.А., Філатов В.О. – К.: КНТЕУ, 2002. – 442с.
2. Макарова М.В., Тенденції розвитку цифрової економіки. // Макарова М.В. – Полтава: РВВ ПУСКУ, 2004. – 235с.
3. Проект Института экономической бзезопасности «Прогноз финансовых рисков» [Електронний ресурс]. – Режим доступу: www.bre.ru/security/21627.html.
4. «Пути решения проблемы безопасности в сфере электронной коммерции» [Електронний ресурс]. – Режим доступу: www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?textid=229 3&level1=main&level2=articles.
5. «Shopping Safely On The Net» [Електронний ресурс]. – Режим доступу: www.police.qld.gov.au/programs/crimePrevention/fraud/online.
6. «Ecommerce risks» [Електронний ресурс]. – Режим доступу: www.tipsforyourwebsite.com/ecommerce_risks.html.
7. «Managing risk in e-commerce» [Електронний ресурс]. – Режим доступу: www.businesslink.gov.uk/bdotg/action/detail?itemId=107538 6132&type=RESOURCES,
8. Miller, Holmes E. and Engemann, Kurt J. (1996); A methodology for managing information-based risk; Information Resources Management Journal; 9:2; 17-24
9. Закон України Про захист від недобросовісної конкуренції (Відомості Верховної Ради (ВВР), 1996, N 36, ст.164) (Вводиться в дію Постановою ВР N 237/96-ВР від 07.06.96, ВВР, 1996, N 36, ст.165) (Із змінами, внесеними згідно із Законами N 642/97-ВР від 18.11.97, ВВР, 1998, N 10, ст. 36 N 783-XIV (783-14) від 30.06.99, ВВР, 1999, N 34, ст.274 - редакція набирає чинності одночасно з набранням чинності Законом про Державний

бюджет України на 2000 рік N 2783-III (2783-14) від 15.11.2001, ВВР, 2002, N 7, ст.51 N 762-IV (762-15) від 15.05.2003).

10. Веллинг Л. Разработка Web-приложений с помощью PHP и MySQL // Веллинг Люк, Томсон Лора, – СПб.: Издательский дом «Вильямс», 2006 – 880с.

УДК 334.78: 330.4: 519.863: 336.64 **В.В. Кокошинський**

Сучасні підходи до формування інтегрованих корпоративних структур

Досліджені: питання поняття, етапи формування та структура інтегрованих корпоративних структур в світі та на Україні, запропонована оптимізаційна модель розподілу інвестицій між підприємствами-членами інтегрованої корпоративної структури.

Ключові слова: *інтегрована корпоративна структура, інвестиції,капітал, інтеграція.*

The questions of notion, stages of forming and structure of the integrated corporate structures in world and in Ukraine are explored, the optimization model of distributing of investments among the enterprises-members of the integrated corporate structure is offered.

Keywords: *an integrated corporate structure, investments, capital, integration.*

Актуальність. В сучасних умовах глобалізації, актуального значення набуває проблема конкурентоспроможності національних суб'єктів господарювання на світових ринках та формування відповідної стратегії економічного розвитку України.

У період активізації в Україні процесів інтеграції як об'єктивного явища особливо актуальною стає проблема формування механізмів і моделей організація