

РОЗДІЛ 3. ТЕОРІЯ І ПРАКТИКА ПОБУДОВИ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

3.1. Моделі електронної комерції. Основи побудови її систем

Як електронна форма взаємодії між економічними контрагентами Е-комерція, додатково до операцій купівлі/продажу, охоплює й можливість супроводу процесів створення попиту на продукцію і послуги, автоматизацію адміністративних функцій, зв'язаних з он-лайнними продажами і обробкою замовлень, а також із вдосконаленням обміну інформацією між партнерами.

Світовий бум електронної комерції, після її виникнення у США, розпочався в 1995-1996-х роках. У 1995-му році була відкрита одна з перших Internet-крамниць Amazon.com.

Роздрібна Internet-торгівля одразу надала покупцям нову якість споживання через наступне:

- замовлення можна було зробити, не виходячи з домівки, завдяки чому економився час;
- закупівля вчинялася в будь-який час доби;
- спектр товарів пропонувався практично не обмежений, бо на відстані одного натиснення мишею знаходилась інша електронна крамниця;
- крамниці одразу почали надавати й інформаційне обслуговування: для споживача завжди була доступна довідкова інформація про товари, а звідси – й можливість співставити товари й ціни;
- система керування електронною крамницею пропонувала індивідуалізоване обслуговування за рахунок “здатності” цього програмного забезпечення “запам’ятовувати” прихилення тисяч користувачів.

Факторами, що сприяли на первинному етапі активному розвитку електронної торгівлі саме у США, були:

- розвиненість он-лайнної культури: у 1995-му році сервіси глобальних національних мереж AOL, CompuServe, Prodigy передплачували близько 15 млн. користувачів;

- сформованість телекомунікаційної інфраструктури;
- розповсюдженість кредитних карток;
- понад 100-річна культура замовлень й продажів за каталогами;
- ефективна робота систем експрес-доставки (DHL, TNT, FedEx та ін.).

В 1996-му році робилося багато прогнозів щодо розвитку Е-комерції. Цікаво поглянути на ці цифри нині, з висоти років, що минули (див. табл. 7).

Очікувані цифри зростання на той час вважалися надмірно оптимістичними, але вже у 1998-му році загальний прибуток від операцій в Internet перевищив 8 млрд. USD, а прибуток від реклами в мережі нині перевищує 2 млрд. USD на рік.

Таблиця 7. Прогнозні показники розвитку електронної комерції, обґрунтовані у 1996-му році

Чинник	1997 рік	2000 рік	Зростання, разів
1	2	3	4
Прибутки від Е-комерції, млрд.. USD	0,3	5	15,67
Загальний обсяг економіки в Internet, млрд. USD	15	200	12,33
Прибуток від реклами американських під мереж, млрд.. USD	0,2	2	9
Кількість компаній, які мають представництво в Internet, %	4	33	7,25

Саме наприкінці 1998 – на початку 1999 року про Internet говорили як про абсолютний ринок, що перевищує за своїм потенціалом будь-який інший у світі. Така постановка проблеми у контексті дослідження уявляється невірною: Internet-ринок не існує як самостійний, подібно до ринку металу, зерна тощо, а є проявом цифрової економіки, місцем реалізації електронного бізнесу.

Реальні обсяги світової Internet-торгівлі, чи електронної комерції за напрямом B2C, у період з 1999-го р. до 2003-го р. на-

ведені на рисунку 22. У 1995-1998 р. р. темпи зростання Internet-торгівлі перевищували темпи зростання сектору B2B.

До 2000-го року основними тенденціями розвитку електронних крамниць були:

- штучне прибільшення капіталізації компанії;
- розкручування бренду;
- залучення відвідувачів будь-якою ціною;
- залучення інвестицій;
- існування он-лайнних крамниць без відповідності їх оф-лайнному, реальному бізнесу.

Катастрофічне падіння акцій Internet-компаній на електронній біржі NASDAQ навесні 2000-го р. призвело до суттєвих структурних змін в електронній комерції (див. рис. 23) й примусило представників цього напрямку електронної комерції переглянути основні підходи до ведення свого бізнесу, а саме:

- привести у відповідність оф-лайнову і он-лайнову діяльність компаній;
- прагнути до підвищення рівня прибутковості фірми за рахунок скорочення витрат й утримання покупців нарощуванням спектру товарів, розширенням сервісів, персоналізацією й підвищенням якості обслуговування [11].

З часом більш показовими й прибутковими, ніж електронні крамниці, стали інші моделі електронної комерції, насамперед, напрямку B2B. Класифікація розповсюджених моделей електронної комерційної взаємодії економічних агентів наводиться нижче.

Моделі електронної комерції. Вже зазначалося (див. підрозд. 2.1), що загальноновизнаними є такі напрями електронної комерції:

- бізнес-бізнес (business-to-business, B2B): визначає взаємодію компаній з іншими компаніями в електронному середовищі;
- бізнес-споживач (business-to-consumer, B2C): визначає взаємодію компаній з кінцевими споживачами в мережі;
- бізнес-адміністрація (business-to-administration, B2A): позиціонує у світі мереж взаємовідносини бізнес-установ і державних органів;

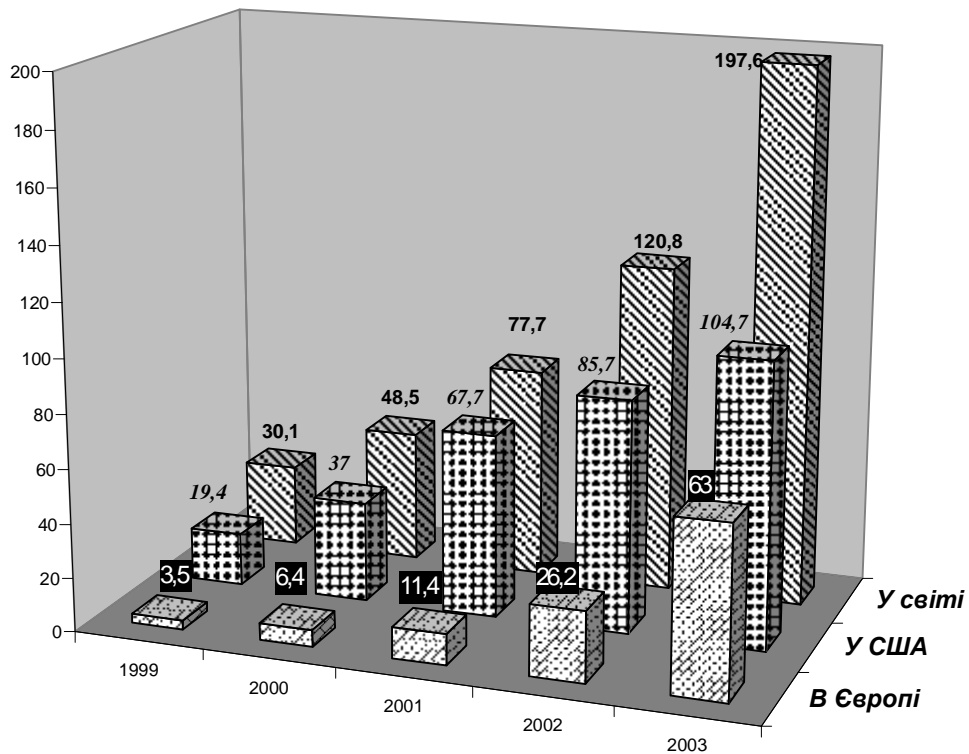


Рис. 22. Світові й регіональні обсяги електронної торгівлі у 1999-2003 р. р. (складено за [11])

- споживач-адміністрація (consumer-to-administration, C2A): окреслює сферу електронної взаємодії фізичних осіб з державою, наприклад, з приводу оплати податків тощо.

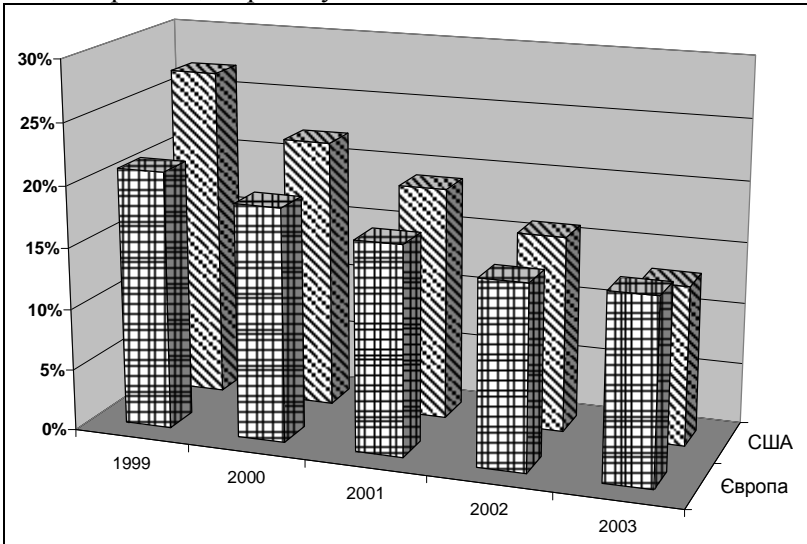


Рис. 23. Доля електронної комерції напрямку B2C в її загальному об'ємі у США і Європі (складено за [11])

За іншими класифікаціями додатково виокремлюються напрями:

- споживач-споживач (C2C – consumer-to-consumer);
- споживач-бізнес (C2B – consumer-to-business);
- бізнес-державна (B2G – business-to-government);
- біржа-біржа (E2E – exchange-to-exchange);
- сумісна комерція.

На практиці додаткові напрями, й ті, назви яких з'являються на сторінках спеціалізованої літератури майже щомісяця, легко зводяться до вже добре відомих. Так, напрям B2A, чи B2G (business-to-government), нічим, крім того, що другим агентом у ланцюжку електронної взаємодії виступає держава, як найсолі-

дніший замовник й покупець у країні, не відрізняється від напрямку B2B.

Розвиток моделей електронної комерції, впровадження пілотних проектів в цій галузі, а також розробка загальних юридичних і правових основ ведення бізнесу в Internet підтримуються Європейською Комісією (ЄК) в ESPRIT та іншими установами. В матеріалах ЄК (www.cordis.lu/esprit/home.html) наводяться визначення і опис одинадцяти моделей електронної комерції. Серед них:

- електронна крамниця;
- електронний каталог-довідник;
- електронний аукціон;
- електронний торговельний центр (мол);
- віртуальне співтовариство;
- віртуальний центр розробки;
- інформаційний брокер;
- провайдер бізнес-операцій;
- інтегратор (посередник) бізнес-операцій тощо.

Авторська класифікація й характеристики моделей за напрямами наведена у таблиці 8.

Моделі електронної комерції напряму B2B (business-to-business). Описують електронну взаємодію між компаніями через Internet. Системи B2B можуть бути відкритими для відвідування звичайними користувачами та іншими можливими партнерами або закритими. Останні існують тільки для певних партнерів чи робочих груп, або ж виконують визначені технологічні функції. Системи електронної комерції B2B забезпечують зв'язок споживачів продукції з її виробниками, покупців з продавцями, однак усі сторони виступають юридичними особами. Новою тенденцією у розвитку систем B2B є напрям керування логістичними ланцюжками (Supply Chain Management), що забезпечує підприємству інформацію про постачання й логістику усіх контрагентів для основного виробництва (дивись підрозд. 2.2).

Модель агрегації – електронного торговельного майданчику, e-marketplace – описує універсальне місце для закупівлі матеріально-технічного забезпечення для компанії, де в єдиному

місці і в єдиному форматі надаються каталоги багатьох постачальників (дивись підрозд. 2.2). Інформація про групи й категорії продукції відображається у режимі реального часу й постійно оновлюється. Зазвичай електронні торговельні майданчики – тематичні й відображають галузеву належність компаній, які користуються їх послугами. Існують торговельні май данчики для компаній агропромислового комплексу, металургійного тощо.

За моделлю *торговельного концентратора* (див. підрозд. 2.2) на сайті утворюються торговельні співтовариства продавців й покупців. Продавцям виділяються місця для реклами своїх товарів, а покупцям надається можливість взаємодіяти з ними з метою отримання новин, специфікацій й описів продуктів.

Горизонтальні торговельні концентратори підтримують усіх продавців й покупців з багатьох галузей промисловості, а діагональні – тільки визначені категорії продавців й покупців з багатьох промислових галузей.

Часто одна операція підприємства містить в собі цілу низку угод, оплат, заліків, інших операцій. У таких господарських ланцюжках зазвичай задіяна велика кількість менеджерів з усіх боків, їх підтримка потребує чимало часу і сил, особливо у керівників, змушених тримати усі деталі ситуації в голові. Автоматизація ж цього процесу на торговельних концентраторах ненабагато складніше, ніж автоматизація окремої угоди. В результаті такий ланцюжок операцій може реалізуватися і контролюватися одним фахівцем.

Модель дошки об'яв або електронного довідника-каталогу передбачає досить складну структуру сайту за категоріями, що дозволяє зацікавленим сторонам після розшуку на ньому необхідної інформації “зустрітися” для переговорів й подальшої взаємодії. Електронні довідники-каталоги застосовуються компаніями для полегшення участі в тендерах, для просування своєї торговельної марки і зниження витрат з маркетингу.

Модель є ідеальним механізмом для взаємодії на сильно фрагментованих ринках з нестандартною продукцією, оскільки усі контракти дуже відрізняються один від іншого й потребу-

ють двосторонніх переговорів. У цій моделі ставиться за мету наблизити підприємства до підпису більш стандартизованих

Таблиця 8. Моделі електронної комерції за основними напрямками

<i>Напрями</i>				
B2B	B2C	C2C	Сумісна комерція	E2E
1	2	3	4	5
Модель агрегації (електронного торговельного майданчика, e-marketplace)	Модель електронної крамниці	Модель он-лайнного споживацького аукціону	Інформаційне обслуговування компаній: <ul style="list-style-type: none"> - довідники; - новини; - посилання на актуальні ресурси й послуги; - стрічка новин; - дискусійні форуми; - календар подій; - інформація про вакансії. 	Модель сукупності Internet-бірж
Модель торговельного концентратора	Модель електронного торговельного центру (електронного молу, E-mall)		Інформаційне обслуговування кінцевих споживачів: <ul style="list-style-type: none"> - дискусійні форуми; - новини; - посилання на актуальні ресурси й послуги; - інформація про вакансії, що 	

Продовження таблиці 8

1	2	3	4	5
			відкриваються, та резюме.	
Модель дошки об'яв	Модель он-лайнного аукціону			
Модель он-лайнних аукціонів: - звичайних; - зворотних.				
Модель цілком автоматичної біржі				
Сумісна комерція компаній: - довідники; - новини; - посилання на актуальні ресурси й послуги; - стрічка новин; - дискусійні форуми; - календар подій; - інформація про вакансії.	-			

контрактів, після чого з'явиться можливість повної автоматизації процесу формування угод.

Модель аукціонів оцінюється як одна з найперспективніших і являє новий варіант ціноутворення для багатьох ринків, де багаточисленні продавці й покупці виставляють конкуруючі замовлення на формування контрактів. Ця модель корисна для ліквідації лишків за найкращими цінами, оскільки потенційні покупці можуть виставляти конкурентоспроможні пропозиції (на підвищення) на закупівлю товарів за ринковою ціною.

Мережні аукціони дають користувачам можливість не тільки реалізувати товари і послуги через Internet, але і здійснити їх тестові продажі. Значна кількість компаній використовують он-лайнкові аукціони як інструмент маркетингової оцінки, з допомогою якого можна визначити розмір початкового попиту і ринкову ціну для нового продукту.

Влаштування роботи віртуальних аукціонів мало чим відрізняється від звичайних. У торгах беруть участь дві сторони – продавець і покупець (покупці). Організатори аукціону найчастіше стягають певну плату за виставлення товару на торги. Для того, щоб брати участь у торгах, користувачу необхідно зареєструватися на сайті, при цьому він заповнює запропоновану йому Web-форму. До неї можуть входити особисті й адресні дані, реквізити пластикової картки тощо.

Он-лайнковий аукціон являє інформаційну базу, в якій містяться описи товарів, що допущені до торгів (лотів). Зазвичай загальний список лотів розбитий на тематичні підкатегорії, що полегшує пошук необхідного товару.

Вибравши бажаний лот, користувач влучає до інформаційного вікна, де він може дізнатися додаткові дані про товар: місцезнаходження продавця і відгуки про нього, номер лота тощо. Там же він може розмістити свою пропозицію. Після цього потенційний покупець несе відповідальність за виконання своїх зобов'язань перед продавцем і організаторами аукціону, насамперед в аспекті своєї платоспроможності. Якщо покупець або продавець не виконує обов'язків, до нього застосовуються певні санкції, такі, як попередження, відвертання від торгів тощо.

Покупцю, який переміг в аукціонних торгах, повідомляється про це електронною поштою або телефоном, при цьому він отримує дані про те, як він може оплатити і отримати куплений товар. Продавець, в свою чергу, отримує повідомлення, в якому вказується, як він може зв'язатися з користувачем, що купив його лот.

Зазвичай, беручи участь в аукціонних торгах, обидві сторони несуть певні ризики, наприклад, покупець може оплатити неіснуючий товар. Для зниження їх рівня рекомендується застосовувати деякі прийоми перевірки надійності свого опонента.

На багатьох он-лайнних аукціонах діє система рейтингових оцінок учасників торгів: переможець аукціону і продавець виставляють друг другу оцінки, які відображають їх ставлення до контрагента, що склалося в процесі взаємодії. Рейтинг є дуже важливим показником, що демонструє надійність і чесність користувача.

Перед укладенням угоди рекомендується встановити контакт з контрагентом, для чого найчастіше вказується адреса електронної пошти, і особисто вирішити всі суперечливі питання.

Почепець і продавець повинні мати уяву про ринкову ціну товару, який купується, інакше, занурившись у конкурентну боротьбу, вони можуть забути про власну зацікавленість, вигоду і встановити занадто занижені ціни або переплатити за товар, який сподобався.

За напрямом зростання чи зменшення ставок он-лайнні аукціони поділяються на звичайні і зворотні (див. підрозд. 2.2). Звичайні ініціюються продавцями: продавець публікує список лотів, що продається, а численні покупці, що беруть участь в аукціоні, пропонують ціну на товар чи послугу, що підвищується. Під час проведення аукціону ціна лота постійно підвищується, а аукціон завершується після визначеного проміжку часу.

Модель звичайного аукціону вигідна для продавця, оскільки дозволяє йому отримати максимальну ціну за товар чи послугу. Мережа підсилює цю вигоду, надаючи змогу прийняти участь в

аукціоні якомога більшої кількості покупців. В результаті проведення аукціону найефективніше визначається ринкова ціна лоту. Ця модель менш вигідна для покупців, оскільки відсутня можливість переговорів між покупцем й продавцем, існує тільки конкуренція між усіма покупцями.

Зворотні аукціони діаметрально відрізняються від звичайних: покупець вказує товар, який би він хотів купувати, а численні продавці конкурують друг з другом, поступово зменшуючи ціну на цей товар. Такий підхід вигідний вже продавцю, особливо якщо необхідний товар пропонується багатьма продавцями: в результаті покупець віддасть мінімальну ціну. При проведенні зворотних аукціонів ціна постійно зменшується, навіть до закриття аукціону.

Модель цілком автоматизованої біржі призначена для стандартизованого ринку товарів широкого споживання. В її межах передбачається наявність пропозицій на закупівлю й продаж з автоматичним співставленням замовлень. В результаті створюється ефективний механізм он-лайнового ринкового ціноутворення.

Бізнес для споживача B2C (business-to-consumer). Нині є найпоширенішим напрямом електронної комерції, спрямованим на прямі роздрібні продажі. Хрестоматійним прикладом тут слугує Amazon.com (www.amazon.com) – найвідоміша у світі американська електронна крамниця з торгівлі книжками, компакт-дисками тощо. Протягом декількох років через неї фактично було зруйновано традиційний букіністичний ринок Америки.

Вважається, що технологія прямих продажів через Internet ефективна для скасування диференціації між великими містами й віддаленими регіонами щодо доступу товарів і послуг для кінцевих споживачів, але за умови вирішених проблем доступу до мережі в регіонах, надійної роботи служб доставки тощо.

Важливою рисою B2C є прямі продажі з мінімальною кількістю посередників. На цю рису цифрової економіки – скасування посередництва, як явища – вже неодноразово зверталася увага в цій роботі. Повна ліквідація посередників надає можливість встановлювати конкурентні ціни на місцях й навіть збі-

льшувати їх, виключаючи відсоток посередників, що призведе до зростання прибутку.

Модель Internet-крамниці – найпоширенішої нині форми електронної комерції – вважається добре опрацьованою й базовою для напряму B2C (дивись підрозд. 2.2).

Принципово поетапна процедура придбання товарів в електронній крамниці на прикладі української торговельної системи Bambook (www.bambook.com.ua) виглядає наступним чином:

- вибір товарів. У крамниці усі товари, що пропонуються, поділені на тематичні розділи: Книги; Музика; Відео; Ігри; Арт; Internet-картки; Сувеніри тощо. Щоб влучити в один з них, необхідно натиснути мишею посилання з назвою розділу, наприклад, Сувеніри. Перед потенційним покупцем з'явиться перелік з фіксованою кількістю товарів активного розділу. Перехід до наступних найменувань здійснюється за посиланнями під списком з попередньою групою товарів, подібно до того, як це відбувається при роботі з Web-сторінкою з результатами запиту до пошукового серверу.

Далі слід обрати товар, який зацікавив. На наступному екрані відвідувач електронної крамниці побачить інформацію про товар (стислу анотацію, ціну, видавництво (для книги) або виробника, вагу, рецензії і відгуки читачів (на книгу)). Якщо прийнято рішення про придбання товару, він включається покупцем до замовлення. Товар автоматично влучає до Кошику покупця – програмного засобу для накопичення відомостей про покупки. Пересуваючись крамницею, можна постійно поповнювати Кошик. Нагорі екрану покупець завжди бачить, скільки товарів в Кошикові і яка загальна сума замовлення. Якщо вже обрані усі потрібні товари, можна переходити до оформлення замовлення;

- формування першого замовлення. Якщо відвідувач електронної крамниці ніколи раніше не робив в неї покупок, він має заповнити картку покупця через Web-форму і продовжити оформлення замовлення.

Заповнена картка містить особисті дані: прізвище, ім'я, по-батькові, контактний телефон, адресу покупця, а також інформацію про зроблені раніше замовлення. Відвідувач крамниці

завжди має доступ до своєї картки і може внести туди будь-які зміни.

На цьому етапі покупець надає продавцю й адресу доставки. Далі крамницею пропонуються можливі засоби доставки замовлення і його оплати, наприклад:

- 1) кредитними картками Visa, MasterCard/Europay, які під час передачі захищені протоколом шифрування SSL. Справжність платіжного сервера тут підтверджена цифровим підписом одного з провідних світових центрів сертифікації відкритих ключів шифрування. Така ж практика є звичайною для будь-якої електронної крамниці. Покупцям рекомендується оформлювати замовлення тільки на прізвище і ім'я власника картки, зазначені в договорі обслуговування і використовувати для оплати замовлень тільки ті номери карт, які видані банком безпосередньо на ім'я власника;
- 2) за рахунком-фактурою в українських гривнях. Така форма оплати доступна юридичним й фізичним особам України. Юридичні особи після роздрукування рахунку-фактури мають перерахувати гроші на розрахунковий рахунок Internet-крамниці; після надходження грошей на рахунок крамниця оформлює відповідні документи і висилає їх разом з замовленням. Фізичні особи перераховують гроші через будь-яке відділення банку або пошти;
- 3) готівкою при доставці замовлення кур'єром;
- 4) за рахунком у доларах США. Цей засіб оплати пропонується для зарубіжних покупців Vambook для проведення банківських переказів.

Нині крамниця пропонує доставку товарів кур'єром за адресою, зазначеному у картці покупця. В примітках картки покупець може вказати час, в який найзручніше отримати замовлення. Доставка більшості позицій усією територією України забезпечується протягом 7-10 робочих днів, у Києві – 3-5 робочих днів з моменту отримання грошей, до інших країн – 7-21 днів. Біля кожного товару в каталозі вказаний термін комплектації замовлення. Для деяких позицій термін доставки становить 20-40 днів.

Після знайомства з запропонованими варіантами покупцю слід зробити свій вибір, виходячи з власних можливостей – чи

має покупець певну банківську картку, чи є він жителем столиці тощо.

Господарі електронних крамниць завжди пропонують новим покупцям передплатити на новини сервера і отримувати в подальшому інформацію про нові надходження до Internet-крамниці, конкурси, вікторини для покупців тощо. Окремо пропонується передплата на новини переглянутих розділів, товари з яких включені до замовлення, про нові надходження до них.

Наприкінці формування замовлення покупець отримує рахунок-фактуру або підтвердження замовлення, в залежності від обраного засобу оплати;

- формування повторного замовлення. Тут від покупця потребується авторизація, тобто введення ним паролю доступу й зазначеної раніше у картці покупця адреси електронної пошти. Далі оформлення замовлення нічим не відрізняється від первинного;
- перегляд замовлень. Після авторизації можна переглянути у картці покупця, посилання на яку присутнє на більшості сторінок крамниці, список і вміст усіх замовлень з датою їх оформлення і номером рахунку-фактури. Замовлення, які мають статус неоплачених, можна анулювати, об'єднати або оплатити;
- отримання знижок при закупівлі. Покупці на сайті www.bambook.com.ua отримують знижки під час оформлення замовлення. Наприклад, програмним забезпеченням електронної крамниці автоматично розраховуються такі знижки на суму кожного замовлення, яке містить три і більше товарів:

100 гривень – 2%;	500 гривень – 5%;
300 гривень – 3%;	1000 гривень – 6%.

Постійним покупцям пропонується знижка, яка буде надаватися на кожне замовлення, незалежно від його суми. Для початку роботи в такому режимі відвідувачу крамниці слід написати повідомлення на адресу адміністрації, яка розгляне листа і відповідь у термін, не більший трьох робочих днів. Щоб стати постійним покупцем з правом на знижки слід, щоб список сплачених за місяць замовлень мав загальну вартість не менше 2000 гривень.

В якісно спроектованих електронних крамницях покупцям обов'язково пропонується функція пошуку потрібних їм товарів.

Так, наприклад, в Vambook організований пошук за найменуванням книги, її автором, видавництвом, за розділом, за ISBN, за ціновим діапазоном й іншим параметрам. Можливий пошук товару як за одним параметром, так одночасно й за декількома.

Також зареєстровані відвідувачі можуть взяти участь у партнерських програмах крамниці, розташувавши на власних Web-сайтах текстові посилання на електронну крамницю і її графічні банери. В Internet-крамниці автоматично реєструються усі замовлення покупців, які потрапили до неї, скориставшись посиланням на сайті покупця-партнера. Причому партнер завжди має можливість відстежити статистику такої реєстрації на сайті електронної крамниці.

Зазвичай наприкінці місяця господарі крамниці підводять підсумки, і партнери отримують свої комісійні, які можуть коливатися у певному діапазоні, наприклад, до 10% від суми замовлень. Партнери можуть обирати форму отримання комісійних: чи грошима, чи товарами з електронної крамниці. Зрозуміло, чим більше товарообіг крамниці, тим суттєво вигідніші партнерські програми з нею.

Партнерські програми електронних крамниць є ще однією яскравою ілюстрацією мережного характеру цифрової економіки, яка ґрунтується на розгалужених мережах складних господарчих взаємовідносин різноманітних агентів.

До п'ятірки товарів і послуг, які найчастіше нині придбаються кінцевими споживачами в електронних крамницях, входять книжки, програмне забезпечення, комп'ютерна апаратура, авіаквитки і різноманітні тури.

У повсякденній роботі електронних крамниць істотною проблемою стало повернення товарів, причому, насамперед у зв'язку з роботою служб доставки й загальною культурою роботи оф-лайнової системи торгівлі. Показовими тут стали численні конфлікти після різдвяних продажів у 2000 і 2001 роках в Америці, пов'язані з поверненням товарів, замовленими через Internet.

Електронний торговельний центр (E-mall, електронний мол) являє Web-сайт, що містить множину електронних крамниць, об'єднаних загальним місцем розташування, інколи під відомою

маркою, які спільно використовують додаткові функції, наприклад, систему проведення захищених платіжних трансакцій.

Новою, перспективною формою Internet-торгівлі вважається модель електронного молу або електронного торговельного центру (E-mall). За своїми властивостями такий Web-сайт схожий на сучасну американську форму оф-лайнної торгівлі у молі, який є скопиченням “під одним дахом” великої кількості різноманітних крамниць із спільної інфраструктурою, своєрідним “містом” крамниць, зорієнтованих на обслуговування покупців певного регіону.

Важливу роль відіграє господар (провайдер) електронного молу, який забезпечує його роботу. Він виконує роль оператора системи і заробляє на продажі програмного забезпечення, здачі в оренду своїх програмно-технічних потужностей і зазвичай не бере участі в бізнесі електронних крамниць. Відкриття крамниці в широко відомому торговельному центрі в Internet надає продавцю надію на велику кількість потенційних покупців і зниження витрат. Крім того, розташування нової Internet-крамниці під відомою маркою забезпечує довіру покупців до нового віртуального торговця і таким чином підвищує готовність покупця не тільки зайти на сайт і переглянути його вміст, але і зробити покупку. Для покупця – це зручний і швидкий доступ до усього співтовариства крамниць, де він використовує єдиний механізм реєстрації і оплати.

Наприклад, Міжнародний центр інформаційних технологій INT нині є провайдером найбільш відомої і реально працюючої вітчизняної системи, яку можна було б класифікувати як електронний мол (www.int-commerce.com). Його проект системи Internet-комерції (CIK) працює при підтримці Національного Банку України. Досить давно функціонує перша і найвідоміша українська торговельна Internet-система – електронний торговельний центр INT-commerce (www.int-commerce.com.ua). До проекту приєдналися електронні крамниці Vambook (торгівля книжками, компакт-дисками), Likon (торгівля медичними товарами), Дукат (торгівля канцелярськими товарами). До системи підключений комерційний банк Аваль. У відвідувачів мола є можливість передплатити в он-лайнні газети і журнали при відвідуванні сайту Київського головпоштамту.

Учасниками СІК ІNT можуть бути:

- покупці, що мають договір з банком-емітентом з обслуговування їх пластикових карток. У молі вони мають усі ті ж можливості, що й покупці звичайної Internet-крамниці, та й додаткові: зі зручного швидкого доступу до усього співтовариства крамниць з використанням єдиного механізму реєстрації і оплати;
- торговці, що мають договір з банком-еквайером з обслуговування пластикових карток і договір з провайдером молу. Вони підтримують в актуальному стані свої електронні каталоги, стежать за правильністю інформації, розташованої в їх Internet-крамницях;
- провайдер електронного молу підтримує апаратно-програмні ресурси доступу для його учасників. Він надає торговцям набір інтерактивних програмних і технічних засобів для впровадження, редагування і управління інформацією про товари і послуги, а також для отримання повної інформації про замовлення і форми оплати замовлень. У разі використання покупцем карткового платіжного інструменту оператор здійснює безпечне транспортування транзакції. Провайдер Е-молу встановлює на майданчикові торговця спеціалізоване обладнання для організації режиму захищеного зв'язку і цілодобово підтримує діяльність Internet-крамниці. Також провайдер надає торговельні, платіжні, адміністративні послуги і сервіси захисту інформації торговцям, несе відповідальність за цілісність і цілість вмісту електронних каталогів торговців. Провайдер зобов'язаний дотримуватися режиму конфіденційності стосовно довірених йому відомостей;
- банк, підключений до Internet через процесінговий центр. Він є обслуговуючим банком-еквайером для торговців щодо платіжних інструментів електронного молу;
- процесінговий центр, підключений до глобальної мережі, який реалізує зв'язок покупців і торговців з платіжними системами.

Мережна взаємодія споживачів з іншими споживачами C2C (consumer-to-consumer). Виокремлюється як напрям електронної комерції, насамперед, завдяки моделі он-лайнного споживацького аукціону. На цьому своєрідному віртуальному торговельному співтоваристві споживачів кожна людина може

купувати й продавати речі. Найвідоміший приклад он-лайнного аукціону C2C – американська компанія американська eBay, з російських слід згадати www.molotok.ru і www.baraholka.ru. За оцінками, сьогодні користувачі мережі здійснюють біля 10% усіх електронних трансакцій на сайті eBay. За думкою Forrester, до 2006 року через споживацькі аукціони буде здійснюватися до чверті усіх он-лайнних трансакцій, решта – через Internet-крамниці, в той час як нині таке співвідношення становить 16 й 84%.

Споживацькі он-лайнні аукціони мають найбільше значення для продажу дорогих товарів, які мають тенденцію до зміни попиту: побутової електроніки, комп'ютерів, іграшок та відеоігор.

Насправді було б невірним відносити подібні аукціони виключно до напрямку електронної комерції C2C, через те, що значна частина B2C-бізнесу здійснюється невеликими компаніями й індивідуальними покупцями, а аукціони є зручним каналом продажів й для них.

Через це електронні аукціони можна вважати універсальною моделлю для декількох напрямів електронної комерції одночасно – B2B, B2C, C2C.

Сумісна електронна комерція. За визначенням Gartner Group є сукупністю електронних засобів, що забезпечують інформаційний взаємозв'язок між корпораціями, їх клієнтами, бізнес-партнерами, постачальниками й співробітниками. Сумісна комерція суттєво розширює межі електронної комерції за рахунок зсунення акцентів з процесів купівлі/продажу на інформаційний обмін між компаніями. Таким чином, сумісну комерцію можна розглядати як різновид електронного бізнесу напрямку B2B для організації інформаційного обміну.

Подібно до сумісної комерції компаній, існує й багато форм інформаційного обслуговування кінцевих споживачів.

Найпоширеніші моделі сумісної комерції:

- *довідники* – Web-сайти, які надають компаніям можливість сумісної роботи у певному секторі ринку. За сутністю є електронними аналогами спеціалізованих журналів, експозицій, конференцій й презентацій, які з часом зможуть замінити ці фі-

зичні механізми. Дозволяють своїм клієнтам створювати власні довідники у визначеному секторі ринку.

- *новини* – модель оперативного надання клієнтам усієї необхідної інформації, що оновлюється, для успішного ведення ними бізнесу у визначеному секторі ринку. Будуються на розміщенні на сайті новин, що постійно оновлюються, наприклад, відомостей щодо доставки товарів для експортно-імпортних ринків.

- *посилання на актуальні ресурси й послуги* призначені для систематизації й підтримки в актуальному стані корисних для певних користувачів посилань на інформаційні ресурси Internet. Наприклад, усі цікаві бізнес-ресурси Uanet постійно актуалізуються на сайті розробника законодавчих довідників – фірми Дінай (www.dinai.ua).

- *стрічка новин* – модель для надання інформації про попит й пропозиції, поточних відомостей про ціни й угоди, а також публікація заголовків новин в реальному часі.

- *дискусійні форуми* надають користувачам можливість взаємодіяти один з одним для обміну досвідом й знаннями про угоди, товари і/або послуги. Такі форуми часто мають вузьку тематичну спрямованість й модеруються фахівцями.

- *календар подій* інформує клієнтів сайту про найвизначніші події у певній галузі. Й нарешті, слід згадати інформацію про вакансії, що відкриваються, та резюме, які корисні й роботодавцям й співробітникам.

Електронна комерція E2E (exchange-to-exchange). Сформувалася, як напрям, після виникнення й широкого розповсюдження Internet-бірж. Розвиток їх взаємодії був об'єктивно зумовлений тим, що на одній Internet-біржі неможливо надати всю різноманітну сукупність товарів й послуг. У зв'язку з цим споживач часто змушений приймати участь в діяльності декількох бірж, що незручно для нього.

В моделі E2E технологія комерції наступна: покупець оформлює замовлення на товар чи послугу на тій електронній біржі, де він зареєстрований; якщо це замовлення не задовольняється

на “своїй” біржі, воно автоматично передається на іншу, доки не буде задоволено.

Основи побудови систем електронної комерції. Створення системи електронної комерції (СЕК), або торговельної Internet-системи (ТІС), часто є першим заходом, з якого для певної компанії починається перехід до ведення бізнесу у мережній формі, що відповідає реаліям й вимогам інформаційного суспільства.

Для її створення спершу слід з’ясувати, яку з ланок вартісного ланцюжка займає компанія, яку частину своїх бізнес-процесів вона хотіла б перевести в електронну форму і які саме сфери діяльності можна оптимізувати, використовуючи Internet-технології.

Тут важлива логічна схема виробничо-комерційних відносин, коли компанія буде бізнес в "прозорій", відкритій економіці. Такий оф-лайновий бізнес природнім шляхом стає основою для он-лайнового. Як вказувалося, виробничі і комерційні відносини достатньо часто з різних причин побудовані нелогічно, вони не відповідають тим умовам, які до них висуває сучасний глобальний ринок. Це є основною причиною невдалого впровадження як внутрішньокорпоративних інформаційних систем, так і СЕК у зарубіжних й вітчизняних компаніях. Бізнес-процеси в будь-якому разі необхідно перебудовувати, щоб вони органічно вписалися до електронної комерції. Інформаційні технології і Internet тут слугують потужним стимулом для перебудови, а в окремих випадках навіть побудови бізнес-процесів, хоча для повного успіху вимагається усвідомлення бізнесменами іманентної відповідності цієї форми вимогам цифрової економіки.

Отже, починати слід з логічної організації бізнес-взаємодії між учасниками торговельного процесу. Тут можна виділити чотири рівня взаємовідносин його учасників, які слугують базою для створення системи електронної комерції, а саме:

1. виробник – дистрибутор;
2. дистрибутор – ділер;
3. дистрибутор – продавець;
4. покупець.

Будь-який з цих рівнів може бути частково або цілком переведений в електронну форму. Компанія має визначити найбільш

вигідне або важливе місце в бізнес-ланцюжку і зробити ставку саме на нього. Якщо, наприклад, виробнику вигідно працювати з дистрибуторами, тому що це найбільш рентабельно, з допомогою системи електронної комерції слід оптимізувати роботу саме з ними.

1. Для компанії-виробника оптимальним варіантом є первинне запровадження торговельної Internet-системи й інші допоміжних засобів електронної комерції до роботи підрозділів збуту продукції компанії.

Для максимального економічного ефекту від впровадження системи електронної комерції, інформаційна система збуту має бути щільно поєднана з системою планування виробництва і системою організації постачань. Таким чином можна мінімізувати цілу низку статей видатків: ТІС дозволяє виключити витрати на оф-лайнні комірні запаси готової продукції, комплектуючих тощо. Про програмні реалізації такого підходу в ERP й CSRP-системах йшлося у підрозділі 2.2.

При формуванні торговельної Internet-системи, її інтерфейсів й інформаційного наповнення розробники мають виходити з орієнтації на певну групу користувачів. Якщо, наприклад, діяльність виробника спрямована на роботу з дистрибуторсько-дилерською мережею, то його ТІС повинна, в першу чергу, привертати увагу її представників.

З іншого боку, часто компанія-виробник створює Internet-крамницю для прямих роздрібних продажів товарів й послуг через Internet. Однак не кожен виробник може собі дозволити прямі он-лайнні продажі через щонайменше дві проблеми.

Перша з них: при переході на прямі електронні продажі компанії доводиться вирішувати питання взаємодії з традиційними дистрибуторсько-дилерськими каналами збуту. Друга проблема полягає в тому, що невеликим виробничим компаніям складно побудувати взаємовідносини з кур'єрськими службами. Послуги великих кур'єрських систем (DHL, TNT тощо) дорого коштують, але вони гарантують високий рівень сервісу у масштабі усього світу. В невеликих кур'єрських компаніях послуги дешевше, але при цьому знижується рівень гарантій доставки товару кінцевим споживачам і охоплення регіонів. Тобто, в першому випадку товар невеликого виробничого підприємства може ви-

явитися неконкурентним за ціною доставки, оскільки обсяги доставки невеликі, а в другому випадку компанії доведеться домовлятися з декількома кур'єрськими службами, що також відіб'ється на кінцевій ціні товару.

Виробник може обмежити зону своїх прямих продажів до локального рівня, наприклад, обслуговувати споживачів в декількох найбільш економічно розвинутих промислових центрах країни й укласти договір з однією-двома кур'єрськими службами. При цьому виробник входить в новий для себе бізнес з взаємодії з системами кур'єрської доставки, хоча раніше працював тільки з великими дистрибуторами. Цей новий бізнес може виявитися для фірми нерентабельним через маленькі обсяги й високі ціни продажів на первинному етапі електронної торгівлі.

2. Ініціатива створення системи електронної комерції на рівні виробник-дистрибутор може виходити й від дистрибутора. Тоді система електронної комерції позиціонується як його Internet-система його постачання. Більшість етапів в її побудові для дистрибутора саме такі, що й для системи збуту виробника. Основним питанням для керівництва дистрибуторської компанії стає вибір альтернативи: чи продавати товар кінцевому покупцю за схемою прямих продажів через Internet, усуваючи з ланцюжка роздрібних продавців, чи продовжувати працювати через дилерів. Рішення з цього питання приймається шляхом моніторингу й аналізу існуючої дилерської мережі з метою визначення найслабкіших місць. Якщо вони є, рекомендується перейти на прямі постачання дистрибутора в цих регіонах.

За будь-яких умов дистрибутору важливо підтримувати й великих дилерів, й початківців. Для останніх перехід на електронно-комерційну систему взаємовідносин може виявитися привабливим і надасть можливість вийти на новий рівень бізнесу.

Можлива й організація електронно-комерційної взаємодії між регіонально розподіленими дистрибуторами, тобто створення реальної мережної системи. В цьому разі на систему електронної комерції покладаються наступні функції:

• Передача дистрибуторами один одному регіонально розподілених замовлень;

• Передача інформації про стан комір, розташованих в різних місцях;

Онадання інформації про роботу системи кінцевим покупцям.

Будь-якому дистрибутору на початку такої діяльності слід визначити його територіальний ареал. Дилером в ланцюжку дистрибутор-дилер може бути регіональний покупець, дрібний гуртовик, можливо, й роздрібна крамниця.

Для дистрибутора основною перевагою електронно-комерційної системи з підтримкою дилерської мережі є усунення проміжних ланок на шляху реалізації товару кінцевому покупцю. Слід ще раз зазначити, що характерною особливістю цифрової економіки є принципова ліквідація у вартісному ланцюжку посередників між виробником товарів й послуг і кінцевим споживачем, через це дистрибуторсько-дилерські мережі також будуть зазнавати в подальшому принципів змін, навіть до їх повного скасування.

3. Організація електронно-комерційної системи "під" роздрібний продаж має свої особливості. Традиційний роздріб вже має ціну на товар, близьку до межових сум. Роздрібному торговцю важко почати займатися прямими постачаннями в інші регіони. Чим більше відстань, тим менше перспектив організувати глобальні прямі постачання. Єдиним винятком тут може бути переведення в електронну форму вже існуючих торговельних мереж.

За сутністю Internet-крамниці мають бути дискаунтерами: в останніх ціни нижче, ніж у звичайних крамницях; весь асортимент товарів зручно розфасований за певними ваговими категоріями; в наявності широке коло порівняно дешевих товарів.

4. Якщо покупець (споживач) – велика організація, холдинг, з допомогою технологій електронної комерції вона, насамперед, може упорядкувати взаємовідносини між партнерами, контрагентами, а також внутрішні корпоративні зв'язки.

Більшість холдингів працюють за схемою взаємних зобов'язань. Навіть якщо холдингові відносини вже побудовані, система електронної комерції надає економію операційних витрат на підтримку функціонування холдингу у зручному і швидкому режимі.

З іншого боку, будь-якій компанії потрібно упорядкувати відносини між суб'єктами компанії – службами збуту, доставки тощо. Електронно-комерційна база надає ефективну базу для та-

кого впорядкування, стимулює реінжиніринг бізнес-процесів компанії тощо.

Таким чином, для компанії найактуальніше в он-лайнній сфері бути адекватною своїм оф-лайнним функціям. Нові канали збуту повинні відповідати існуючому бізнесу.

Створення торговельної Internet-системи, як й будь-якої іншої інформаційної системи компанії, починається з опрацювання питань організації її бізнес-схеми і розробки проектного завдання. У ньому відбиваються питання взаємодії під час проведення електронних операцій господарюючих агентів, що входять до торговельного процесу. Наприклад, виробнику слід домовлятися з кожним з дистрибуторів про перехід на нові для них форми електронно-комерційної взаємодії, укладати з ними додаткові договори, навчати новим засобам ведення бізнесу, надавати інформаційні матеріали. Уся низка цих питань має бути відбита в проектному завданні.

При створенні СЕК практикуються такі організаційні заходи:

- виокремлення Internet-торговельного проекту в самостійну організаційну структуру, навіть в автономну юридичну особу. Матрична структура, коли для участі в проекті призначаються співробітники з різних підрозділів, у цьому разі неефективна. Internet-проект повинен мати власних менеджерів: логістика, фахівця з постачання і збуту та інш., які будуть цілком зорієнтовані на Internet-технології;
- забезпечення прямої підпорядкованості Internet-проекту керівництву компанії;
- очолення проекту керівником, який добре розуміється на основному бізнесі компанії і приймав участь в управлінні цим бізнесом. Необов'язково, щоб він був експертом в галузі інформаційних технологій і Internet;
- формування для проекту команди бізнес-експертів, які можуть впливати на прийняття рішення і вибір технологій, спираючись на рекомендації IT- і Internet-фахівців.

Успішна електронна комерція передбачає наявність підтримуючих механізмів, котрі мають як спільні риси в глобальному масштабі, так й національні особливості. До їх складу входять системи проведення електронних платежів, служби доставки то-

варів, правові й технічні механізми захисту комерційної інформації в мережі, рекламні й маркетингові заходи та інш.

3.2. Механізми підтримки Е-комерції

3.2.1. Системи платежів для електронної комерції

Необхідність платіжних Internet-систем. Умови проведення електронних платежів. Платіжна Internet-система призначена для проведення розрахунків між фінансовими установами, бізнес-організаціями і Internet-користувачами під час купівлі/продажу товарів і послуг через глобальну мережу. Саме електронна платіжна система дозволяє перетворити службу з обробки замовлень або Web-вітрину компанії в повноцінну електронну крамницю з усіма стандартними атрибутами: вибравши товар або послугу на сайті продавця, покупець може здійснити платіж, не відходячи від комп'ютера.

Електронні платіжні системи є найважливішим механізмом підтримки проведення комерційних операцій з допомогою комп'ютерних мереж. Прозорі для клієнтів принципи їх побудови й функціонування є однією з запорук успіху електронної комерції у будь-якій країні. Проблематиці виникнення і формування систем проведення платежів в Internet присвячені роботи як зарубіжних дослідників (Б. Уолш [16]), так й українських і російських авторів (Л. А. Пономаренко [3], С. Волков [10], [13], В. Достов [13], О.В. Бойчун [9]).

В системі електронної комерції платежі вчиняються при додержанні низки умов:

- забезпечення конфіденційності: при проведенні платежів через Internet покупець бажає, щоб його ідентифікаційні дані, наприклад, номер кредитної картки, були відомі тільки установам, які мають на це законне право;
- збереження цілісності інформації про купівлю: її ніхто не може змінити;

- проведення аутентифікації: покупці і продавці мають бути впевнені, що усі сторони угоди є тими, за кого вони себе вдають;
- забезпечення багатоваріантності засобів оплати: можна платити усім доступним покупцю;
- проведення авторизації – процесу, під час якого вимога на проведення трансакції схвалюється або відхиляється платіжною системою, що дозволяє визначити наявність коштів у покупця;
- гарантії ризиків продавця, наприклад, пов'язаних з відмовами від товару і несумлінністю покупця. Їх величина має бути узгоджена з власником, чи провайдером, електронної платіжної системи й іншими учасниками торговельних ланцюжків шляхом спеціальних угод;
- збереження таємниці;
- мінімізації плати за трансакцію: плата за обробку трансакцій замовлення і оплати товарів входить до їх вартості, тому зниження її ціни збільшує конкурентоспроможність продавців. Трансакція має бути оплачена в будь-якому випадку, навіть при відмові покупця від товару.

Класифікація і характеристика платіжних Internet-систем. Усі платіжні B2C Internet-системи за наявною схемою платежів можна поділити на:

◆ дебетові, що обслуговують роботу з електронними чеками і цифровою готівкою;

◆ кредитні, для роботи з кредитними картками.

Перші поширені менше, але найцікавіші з точки зору їх перспективності, особливо схеми з цифровими грошима на смарт-картках. Дебетові схеми платежів побудовані подібно до їх офлайн-прототипів – чекових і звичайних грошових. До схем включені дві незалежні сторони: емітенти – суб'єкти, що керують платіжною системою, і користувачі. Перші випускають електронні одиниці для обслуговування платежів, наприклад, гроші на рахунках в банках. Користувачі систем вчиняють і приймають платежі в Internet з допомогою випущених електронних одиниць.

Перший різновид *дебетових Internet-систем* – *електронні чеки*, що подібні до звичайних паперових чеків – доручень плат-

ника своєму банку перерахувати гроші з його рахунку на рахунок одержувача платежу – продавця. Відзнаки полягають у тому, що, по-перше, виписуючи паперовий чек, покупець ставить свій реальний підпис, а в он-лайнному варіанті – підпис електронний. По-друге, самі чеки видаються в електронному вигляді. Проведення платежів минає в декілька етапів (див. рис. 24):

1. платник видає електронний чек, підписує його електронним підписом і пересилає продавцю;
2. чек подається до оплати платіжній системі. Або тут, або в банку одержувача платежу відбувається перевірка електронного підпису;
3. у випадку підтвердження її справжності постачається товар або надається послуга. З рахунку платника (покупця) гроші перераховуються на рахунок продавця.

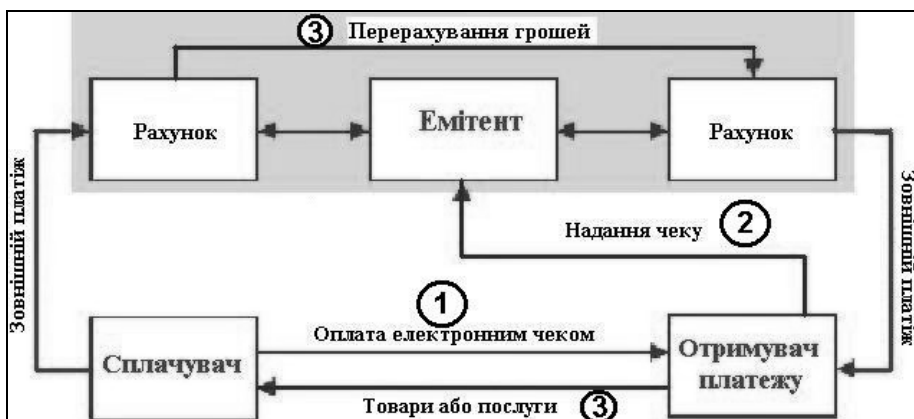


Рис. 24. Проведення платежів електронними чеками

Простота схеми проведення платежів, на жаль, нівелюється труднощами її впровадження в пострадянських СНД. Тут, на відміну від інформаційно розвинутих країн, чекові схеми поки не отримали розповсюдження через відсутність розвинутої національної системи сертифікаційних центрів – установ для видачі й зберігання цифрових сертифікатів – засобу для підтвердження дійсності електронних підписів.

Сертифікаційні центри відіграють найважливішу роль у коректному функціонуванні платіжних електронних систем і є розвинутими інститутами у західних й південноазійських інформаційних суспільствах.

Для реалізації електронного підпису використовують систему шифрування з відкритим ключем (ВК). При цьому створюється особистий ключ для підпису і ВК для перевірки. Особистий ключ зберігається у користувача, а відкритий може бути доступний усім. Найзручніший спосіб розповсюдження ВК – використання сертифікаційних центрів. Там зберігаються цифрові сертифікати, які містять відкритий ключ і інформацію про власника. Це звільняє користувача від обов'язку самому розсилати свій ВК. Крім того, сертифікаційні центри забезпечують аутентифікацію, яка гарантувала б, що ніхто не зможе згенерувати ключі від іншої особи.

У *дебетових платіжних системах з цифровою готівкою* емітент випускає електронні аналоги реальних грошей. Вони придбаються користувачами для оплати куплених товарів і послуг, після чого продавець погашає їх у емітента. При емісії кожна грошова одиниця засвідчується електронною печаткою, яка перевіряється структурою, що їх випустила перед погашенням.

Одна з особливостей реальних грошей – їх анонімність. Деякі електронні платіжні системи з допомогою схеми “сліпих” підписів дозволяють покупцю отримувати цифрову готівку так, щоб не можна було визначити зв'язок між ним і грошима. При використанні електронних грошей також немає необхідності в аутентифікації, оскільки система заснована на випуску грошей в обіг перед їх використанням. За такої схеми (див. рис. 25):

1. покупець заздалегідь обмінює реальні гроші на електронні. Вони можуть зберігатися у клієнта двома способами, що визначається певною платіжною системою: ♦ на жорсткому диску комп'ютера; ♦ на смарт-картках. На жаль, псування диску або смарт-картки обертається втратою електронних грошей.

Пропонуються різні схеми обміну реальних грошей на електронні. Часто відкриваються спеціальні рахунки, на які перерахо

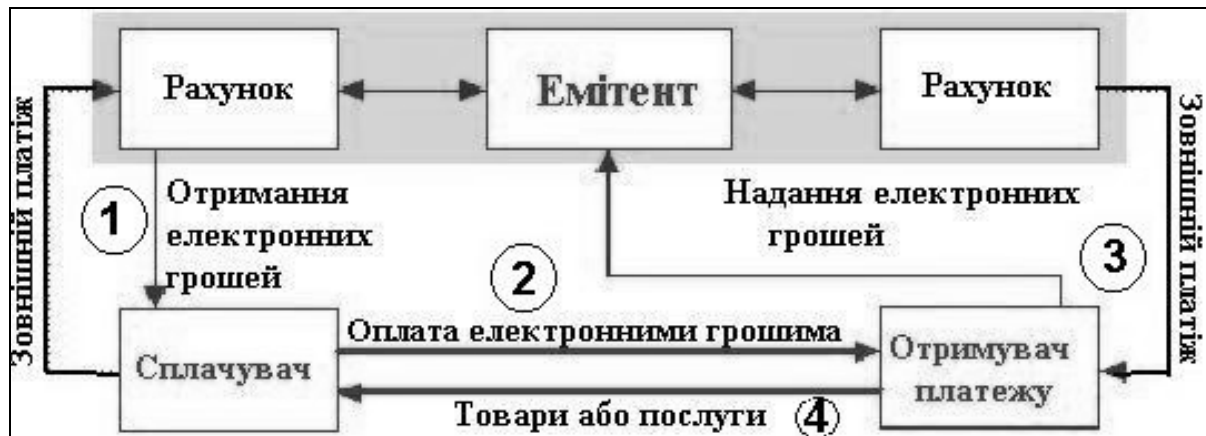


Рис. 25. Схема платежу з допомогою цифрових грошей

вуються кошти з рахунку покупця в обмін на електронні купюри. Деякі банки самі можуть бути емітентами електронної готівки за запитом клієнта з її наступним перерахуванням на його комп'ютер або смарт-картку і зняттям грошового еквіваленту з особистого рахунку.

За умови реалізації “сліпого” підпису покупець власноручно створює електронні купюри: генерує у певній програмі рядки літер і цифр у звичайному вигляді, які містять номінал, скажімо, 1000 гривень або доларів; у кожній купюрі є індивідуальний серійний номер, відомий тільки покупцю. Потім покупець “запаковує” частину купюри з серійним номером у “цифровий конверт” і пересилає їх до банку чи іншого емітенту. Цифрові купюри поки ще не мають вартості, і привласнити її здатний тільки емітент. Він перевіряє номінали пересланих покупцем купюр, але не в змозі визначити їх закриті серійні номери. Емітент підписує своїм “сліпим” підписом купюри, знаючи їх номінали, але не серійні номери, і повертає покупцю вже засвідченими. Процедура здійснюється за умови надходження реальних грошей на рахунок клієнта. Таким чином, покупець отримує електронні гроші з визначеною, підтвердженою вартістю, якими вже можна оплачувати товари і послуги. При цьому забезпечується повна анонімність платежу;

2. покупець перераховує на сервер продавця електронні гроші за придбаний товар або послугу;
3. гроші надаються емітенту, який перевіряє їх справжність;
4. у випадку справжності електронних купюр рахунок продавця збільшується на суму купівлі, а покупцю відвантажується товар або надається послуга.

Цифрові гроші забезпечують можливість вчиняти мікроплатежі: номінал купюр може не відповідати реальним монетам, наприклад, 48 копійок. Мала вартість транзакції робить електронну готівку привабливим інструментом платежів в Internet.

Емітувати електронну готівку можуть як банки, так і небанківські установи. Однак, у світі й досі не вироблена єдина система конвертування різних типів електронних грошей. Через це тільки самі емітенти можуть гасити випущену ними електронну готівку. До того ж, використання подібних грошей від емітентів-нефінансових структур не забезпечене гарантіями з боку дер-

жав. Загальновідомими системами цифрової готівки нині є: CyberCash і DigiCash.

Світова система, заснована на використанні смарт-карток – Mondex – належить відомому емітенту MasterCard з 1996-го р. Ця технологія перетворює гроші ще в один різновид готівки. Гроші емітуються на картку власника, а потім знімаються у місцях продажів, переносяться з картки на картку і, теоретично, приймаються в будь-якій країні світу, яка приєдналася до системи Mondex. Гроші, виплачені у Mondex, на відзнаку від усіх інших смарт-систем, не авторизуються. Анонімність платежу повна, що і є головною відзнакою готівки. На жаль, у багатьох країнах поки заборонені великі анонімні платежі.

Відзнака *кредитних електронних платіжних систем* від звичайних полягає в проведенні всіх транзакцій через Internet і, внаслідок цього, в необхідності додаткових засобів безпеки і аутентифікації.

В проведенні платежів через Internet з допомогою кредитних карток беруть участь:

1. покупець;
2. банк-емітент, що обслуговує розрахунковий рахунок покупця. Він випускає картки і є гарантом виконання фінансових зобов'язань клієнта;
3. продавець;
4. банки-еквайєри, які обслуговують продавців. Кожний продавець має єдиний банк, в якому він тримає розрахунковий рахунок;
5. платіжна Internet-система – електронні компоненти, що є посередниками між іншими учасниками платіжної системи;
6. традиційна платіжна система – комплекс фінансових

і технологічних засобів для використання банківських карток певного типу як засобів платежу за товари і послуги, проведення взаємозаліків тощо. Учасниками системи є фізичні і юридичні особи, об'єднані відносинами з використання кредитних карток;

7. процесінговий центр платіжної системи – установа, що забезпечує інформаційну і технологічну взаємодію між учасниками традиційної платіжної системи;

8. розрахунковий банк електронної платіжної системи – кредитна установа, що здійснює взаємозаліки між її

учасниками за дорученням процесінгового центру.

Найпоширеніша нині схема платежів в таких системах наведена на рис. 26:

1. покупець в електронній крамниці формує кошик товарів і обирає засіб оплати кредитною картою;

2. далі параметри кредитної картки: номер, ім'я власника, дата закінчення чинності тощо мають бути передані платіжній системі Internet для подальшої авторизації. Це відбувається двома шляхами:

- параметри картки вводяться на сайті крамниці, після чого вони передаються платіжній системі Internet;
- параметри картки вводяться на сайті електронної платіжної системи.

Зрозумілі переваги другого шляху: відомості про картку не залишаються в електронній крамниці, і, відповідно, знижується ризик отримання їх третіми особами або шахрайства продавців. Однак в обох випадках все ж існує можливість перехвату шахраями реквізитів кредитної картки в мережі. Для відвертання цього зв'язки типу покупець/продавець, продавець/платіжна Internet-система, покупець/платіжна Internet-система здійснюються у шифрованому вигляді з допомогою захищених протоколів. Найбільш розповсюджені протоколи SSL (Secure Sockets Layer) і SET (Secure Electronic Transaction) (див. підрозд. 3.2.2).

3. платіжна Internet-система передає запит на авторизацію традиційній платіжній системі;

4. наступний крок залежить від того, чи підтримує банк-емітент он-лайн базу даних рахунків. За її наявності процесінговий центр передає банку-емітенту запит на авторизацію картки й отримує його результат. Якщо такої бази немає, то процесінговий центр самий зберігає відомості про стан рахунку власників карток, стоп-аркуші і виконує запити на авторизацію. Ці відомості регулярно оновлюються банками-емітентами;

5. результат авторизації передається платіжній Internet-системі;

6. електронна крамниця одержує результат авторизації;

7. покупець отримує результат авторизації через крамницю або безпосередньо від платіжної Internet-системи;

8. при позитивному результаті авторизації:

Рис. 26. Схема платежів через Internet з допомогою кредитних карток

- електронна крамниця надає послугу або відвантажує товар;
- процесінговий центр передає в розрахунковий банк відомості про здійснену транзакцію. Гроші з рахунку покупця в банку-емітенті перераховуються через розрахунковий банк на рахунок крамниці в банку-еквайєрі.

На практиці за такою схемою платежу на шляху від покупця до продавця часто виникає нагромадження всіляких додаткових структур, які називають себе фінансовими операторами, процесінговими і препроцесінговими компаніями, авторизаційними центрами тощо. І чим сильніша заплутаність законодавства в країні, тим більша кількість таких структур задіяна в механізмі електронної комерції, і тим далі електронна комерція від кінцевого споживача. У подібних західних системах вони також присутні, але їх в ланцюжку принципово менше. Основна проблема такого підходу, властивого для вітчизняних форм реалізації електронної комерції, – в його заплутаності і складності розуміння кінцевим споживачем, і як наслідок – його недовіра і гальмування прогресу в цій області.

Електронні платіжні системи в українському і російському сегментах Internet. За маркетинговими дослідженнями, в більшості випадків Internet-крамниці у вітчизняному сегменті мережі реалізують товари через кур'єрів, і електронні платіжні системи їм поки не дуже корисні у зв'язку з низькою інформованістю споживача про них. Збільшити зацікавленість покупців можна тільки спільними зусиллями власників електронних платіжних систем і Internet-крамниць.

Електронні платіжні системи цифрової готівки. PayCash і Webmoney Transfer характеризуються їх провайдерами як системи цифрових грошей, однак це більш вірно для системи PayCash. Її власники – банк "Тавричеський" і група компаній "Алкор-Холдинг" – при формуванні системи використали документи Базельського комітету з банківського нагляду. Виходячи з них, PayCash була створена, як анонімна, безпечна – за умови повної недовіри усіх учасників один одному, симетрична – з допомогою електронних грошей можна і платити, й отримувати платежі. У кожного користувача системи програмним шляхом відкривається "електронний персональний гаманець" з цифро-

вими грошима. Покупець робить замовлення в електронній крамниці, ініціюється “гаманець”, продавець висилає покупцю контракт в електронній формі. Далі усе відбувається за наведеною вище схемою (див. рис. 22).

Вузьким місцем системи є неможливість перерахування грошей покупців до PayCash з кредитних карток. Це пов’язано з тим, що компанії-емітенти картокових систем забезпечують своїм клієнтам можливість відмови від здійснення платежу числом, що минуло, – charge back. Це захищає власника кредитної картки від шахраїв. У разі такої відмови вартісне підтвердження доказу того, що товар був наданий дійсному власнику кредитної картки й що платіж має бути здійснений, лягає на продавця. У PayCash такий доказ принципово неможливий. Щоб зробити більш зручним для клієнтів переказ реальних грошей, PayCash забезпечила прийом платежів через систему переказів Contact, де тарифи значно нижче поштових (2,2% против 8%), і скретч-картки, що розповсюджуються у вільній торговельній мережі.

Нині ця платіжна система представлена в Росії, США, деяких інших країнах. Її представництво відкрито і в Україні (www.paycash.com.ua), з 2003 року – під торговельною маркою “Internet-деньги” (www.imoney.com.ua). Для будь-якої операції PayCash визначена договірна база, заснована на Цивільному Кодексі країн, на які розповсюджується дія цієї платіжної системи.

Система Webmoney Transfer – піонер на ринку електронних платежів у країнах СНД – нині має широке міжнародне представництво, в тому числі, й в Україні (www.webmoney.com.ua). В системі два учасника, що забезпечують її ліквідність: NTV Online Banking і автономна некомерційна організація “ВМ Центр”.

Режим функціонування Webmoney нагадує роботу з цифровою готівкою, але не забезпечує повної анонімності платежів, бо вони не є закритими від власників системи. Система дозволяє користувачам відкривати рахунки і переказувати кошти у двох валютах: карбованцях і доларах, а в Україні і в гривнях. Для доступу до системи також використовується “електронний гаманець”. Зараховувати гроші можна банківським й небанківським переказами, через скретч-картки.

Електронна платіжна система змішаного типу. CyberPlat об'єднує три складові: класичну систему "клієнт-банк"; систему CyberCheck для захищених розрахунків між юридичними особами у секторі B2B; систему CyberPos для обробки платежів з кредитних карток у секторі B2C. CyberPlat забезпечує роботу з великою кількістю різновидів кредитних карток: Visa, Mastercard/Eurocard, American Express⁷, Diners Club, JCB, Union Card тощо.

Для фізичних осіб вона має два платіжних інтерфейси. Перший передбачає наявність у банку "Платина" банківського рахунку клієнта. Покупець реєструється в системі і копіює на свій комп'ютер через Internet програмне забезпечення, водночас реєструючись в банку "Платина", як фізична особа. Йому відкривається рахунок, на який клієнт переказує гроші. Після замовлення ним товарів на сайті Internet-крамниці, її власники з допомогою програмного інтерфейсу виставляють покупцю рахунок з проханням підтвердити його. Після підтвердження рахунку під ним формується цифровий підпис покупця, і рахунок вирушає в банк на авторизацію. Якщо все відповідає запитам, крамниця і покупець одержують підтвердження авторизації і гроші переказуються з рахунку покупця на рахунок крамниці, здійснюється доставка товару. Незважаючи на характеристику цього механізму як звичайного "клієнт-банк", у ньому є елементи автоматизації підготовки платежів.

Другий платіжний інтерфейс працює з кредитними картками міжнародних платіжних систем. Ця схема не вимагає попередньої реєстрації покупця в системі. Покупець, заходячи на сайт електронної крамниці, що обслуговується у CyberPlat, формує кошик товарів і пересилається на авторизаційний сервер, де він вводить реквізити картки. Після проведення авторизаційної транзакції для платіжних карткових систем відповідь транслюється і покупцю, і крамниці. За цією схемою здійснюється 99% транзакцій.

Окрім вищеописаних платіжних Internet-систем, на вітчизняному електронному ринку пропонуються й інші механізми. Наприклад, кліринг: замкнуті у межах спілок провайдерів Internet платежі між їх клієнтами. Принцип такої платіжної системи по-

лягає у перерахування коштів з рахунку клієнта А у провайдера на рахунок клієнта В у того чи іншого провайдера, а не в банку.

Різноманітність фінансових механізмів проведення платежів за комерційні операції масових споживачів у глобальній мережі лише підкреслює їх багаті можливості. На жаль, електронні платіжні системи не отримують достойного розповсюдження в Uanet і Runet через декілька причин. Це:

- й недостатня поки кількість користувачів мережі, а звідси – й потенційних споживачів послуг електронної комерції та її платіжних систем;
- невисока інформаційна культура населення пострадянських країн, в тому числі, й українського, низький рівень його інформованості про електронні платіжні засоби і через це – неспроможність користуватися ними;
- низький рівень розповсюдженості традиційних кредитних карткових систем і недовіра нашого населення до них;
- низький платіжнеспособний попит населення на товари взагалі й товари, що пропонуються через систему Е-комерції.

3.2.2. Проблеми безпеки і захисту комерційної інформації в Internet

Ймовірні загрози небезпеці інформації в мережі і рішення з її захисту. Експоненціальне зростання користувачів Internet в останні роки призвело до появи у мережі тих самих негативних порядків, що неминуче встановлюються у будь-якому людському натовпі. Покупки товарів за чужими кредитними картками, крадіжки інтелектуальної власності в Internet придбали величезні масштаби.

Основною проблемою безпеки електронної комерційної взаємодії в Internet з моменту її виникнення була проблема передачі закритої інформації: номерів кредитних карток, сум платежів тощо через відкриту мережу.

Ймовірні загрози небезпеці інформації, що передається в мережі, разом з рішеннями, які дозволять організувати і значно підвищити захищеність даних, наведені у таблиці 9.

Таблиця 9. Ймовірні загрози небезпеці інформації в мережі і рішення з її захисту

№ з/п	Різновид загрози	Рішення	Дія	Технологія
1	2	3	4	5
1.	Дані навмисно перехоплюються, читаються або змінюються	Шифрування	Кодування даних, яке перешкоджає їх читанню або викривленню	Симетричне або асиметричне шифрування
2.	Користувачі ідентифікують себе невірно, з шахрайською метою	Аутентифікація	Перевірка справжності відправника, одержувача і повідомлення	Цифрові підписи
3.	Користувач отримує несанкціонований доступ з однієї мережі до іншої	Брандмауер	Фільтрація трафіку, який йде до мережі або на сервер	Брандмауери, віртуальні приватні мережі (VPN, Virtual Private Network)

Найбільш поширеною є крадіжка ідентифікаційної інформації, коли злодії збирають персональну інформацію – імена, адреси, номери соціального страхування й інші важливі дані, а після цього замовляють картки під цими іменами. Хоча крадіжки такого типу не новина, Internet значно полегшив їх здійснення. Хакери і кракери “зламують” сайти з такою інформацією. В деяких випадках злочинці удають з себе легітимних он-лайнних торговців і збирають інформацію у покупців, які нічого не підозрюють.

Дійсні номери карток також можуть бути автоматично згенеровані. Internet перенасичений хакерськими сайтами, які пропо-

нують програмне забезпечення для генерації номерів кредитних карток, що здаються дійсними. Ці програми використовують складний алгоритм створення номерів, в яких перші чотири цифри відповідають дійсним цифрам банків-емітентів. Генератори створюють 12 додаткових цифр, які при перевірці відповідають параметрам дійсних карток. Навіть, якщо жодний банк ніколи не емітував картку з цим згенерованим номером, може статися, що вони будуть авторизовані при електронних платежах. Часто кредитні картки викрадаються у реальному світі і використовуються для он-лайнних закупівель.

Важливість проблеми шахрайства з кредитними картками в Internet часто неоднозначно оцінюється різними агентами електронної комерції. Насамперед згадується про загрозу для безпеки споживачів, однак, наприклад, ризик американських мережних покупців досить невеликий: за федеральними законами, їх максимальна відповідальність обмежується 50 USD, хоча це не зупиняє кредитні асоціації від експлуатації фобії шахрайства при просуванні різноманітних "схем захисту".

Від реального ризику потерпають продавці, саме вони несуть головну відповідальність за шахрайські он-лайнні трансакції. Співвідношення шахрайства такого типу становить від 2% продажів в одних товарних категоріях, до 40% – в інших. Наприклад, такий гігант електронної комерції, як Amazon.com визнає серйозність цієї проблеми і заявляє, що його спроможність протистояти шахрайству з боку третіх сторін, що вчиняється шляхом трансакцій з допомогою кредитних карток, є одним з ключових чинників, які впливають на результати діяльності компанії.

Рівень шахрайства у два відсотки перевищує оцінки компаній Visa і MasterCard – найвідоміших емітентів кредитних карток – в двадцять разів. У роздрібному бізнесі 2% продажів можуть складати половину прибутку компанії. Крім того, постраждали продавці платять штраф за кожне повернення, відшкодування володарю картки за неавторизований продаж. Якщо повернення стають частими, продавець сплачує підвищену комісію за трансакції або втрачає цю послугу взагалі.

Шахрайські замовлення в мережі можна поділити на дві категорії: це закупівля товарів, що можна легко обміняти на наяв-

ні, і трансакції, які не вимагають фізичної доставки. До першої категорії влучають такі товари, як споживча електроніка, діаманти і презентаційні сертифікати. До другої – програмне забезпечення, яке можна завантажити з мережі, і передплата на сайти "для дорослих". На останніх, щонайбільше, американських практично 100% трансакцій з деяких країн Східної Європи є шахрайськими.

Як зазначалося, головними вимогами до проведення комерційних операцій в Internet є конфіденційність, цілісність, аутентифікація, авторизація, гарантії (неможливість відмови) і збереження таємниці. Перші чотири вимоги можна забезпечити технічними засобами, але виконання останніх двох – досягнення гарантії і збереження таємниці – залежить й від технічних засобів, й від відповідальності окремих осіб і установ, а також від дотримання законів, що захищають споживача від можливого шахрайства.

Для аутентифікації і збереження таємниці в мережі використовується *шифрування*. Ідентифікація, як різновид аутентифікації, перевіряє, чи є відправник повідомлення тим, за кого себе видає. Аутентифікація ж перевіряє не тільки особистість відправника, але і відсутність змін в повідомленні. Збереженням таємниці є захист повідомлень від несанкціонованого перегляду.

В основі шифрування лежить два поняття: алгоритм і ключ. Криптографічний алгоритм – математична функція, яка комбінує відкритий текст або іншу зрозумілу інформацію з ланцюжком чисел, що називаються ключем, для того, щоб в результаті був отриманий незв'язний шифрований текст. Алгоритм і ключ – основа процесу шифрування. Новий алгоритм важко придумати, але один алгоритм можна використовувати з багатьма ключами. Існують також деякі спеціальні криптографічні алгоритми, які не використовують ключі.

Нині розповсюджені такі алгоритми шифрування:

- DES (Data Encryption Standard) – шифр, розроблений фахівцями фірми IBM і затверджений урядом США у 1977 році. Використовує закритий 56-бітовий ключ і оперує блоками даних по 64 байт. Відносно швидкий, застосовується при одноразовому шифруванні великої кількості даних;

- потрійний DES заснований на DES. Шифрує блок даних три рази трьома різними закритими ключами. Запропонований в якості альтернативи DES, оскільки загроза швидкого і легкого зламу останнього швидко зростає;
- RC2, RC4, RC5 – шифри із змінної довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Ці алгоритму діють трохи швидше DES і здатні підвищувати ступінь захисту за рахунок вибору більш довгого ключа. RC2 – блочний шифр, його можна застосовувати як альтернативу DES. RC4 являє собою потоковий шифр і працює майже в десять разів швидше DES;
- IDEA (International Data Encryption Algorithm) створений у 1991 році і призначений для швидкої роботи в програмній реалізації. Дуже стійкий шифр, який використовує 128-бітовий закритий ключ;
- RSA названий на честь його розробників (Rivest, Shamir і Adelman). Алгоритм з відкритим ключем підтримує змінну довжину ключа шифрування, а також змінний розмір блоку тексту, що шифрується. Розмір блоку відкритого тексту повинен бути менше довжини ключа;
- DSA (Digital Signature Algorithm) може створювати підписи швидше RSA. Пропонується за якості стандарт цифрового підпису (Digital Signature Standard, DSS).

Найдавніша форма шифрування з використанням ключа – симетричне шифрування або шифрування з таємним ключем. При шифруванні за такою схемою відправник і одержувач володіють тим самим ключем, з допомогою якого і той, і інший можуть зашифрувати і розшифрувати інформацію.

Схемам симетричного шифрування притаманні проблеми з аутентифікацією, оскільки особистість відправника або одержувача повідомлення гарантувати неможливо. Якщо двоє володіють одним ключем, кожен з них може написати і зашифрувати повідомлення, а після цього заявити, що це зробив інший.

Така невизначеність не дозволяє реалізувати принцип неможливості відмови. Проблема відмови від авторства дозволяє вирішити криптографія з відкритим ключем, що використовує асиметричні алгоритми шифрування.

У симетричному шифруванні використовується один секретний ключ для шифрування і розшифрування повідомлень.

Криптографія з відкритим ключем заснована на концепції ключової пари. Кожна половина пари ключів шифрує інформацію таким чином, що її може розшифрувати тільки інша половина. Перша частина ключової пари – особистий ключ – відома тільки її володарю. Інша половина – відкритий ключ – розповсюджується серед усіх його респондентів, але зв'язана тільки з цим володарем. Ключові пари володіють унікальною властивістю. Дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари.

Відкрита частина ключової пари може вільно розповсюджуватися без побоювань, що це завадить використанню особистого ключа. Ключі можна використовувати і для забезпечення конфіденційності повідомлення, і для аутентифікації його автора.

Слід враховувати, що кожний, хто має копію особистого відкритого ключа користувача, здатний прочитати повідомлення, зашифроване ним. У комерційних транзакціях прийнята стандартна процедура: покупець шифрує повідомлення своїм особистим ключем, а підтвердження продавця, в свою чергу, шифрується його особистим ключем. Це означає, що будь-хто, кому відомий відкритий ключ продавця, спроможний це підтвердження прочитати. Для збереження в таємниці інформації, посланої продавцем, необхідні додаткові кроки.

Оскільки певний користувач – єдиний, хто має можливість зашифрувати яку-небудь інформацію своїм особистим ключем, будь-хто інший, хто використовує його відкритий ключ для розшифрування повідомлення, може бути впевнений, що воно від цього користувача. Таким чином, шифрування електронного документа користувача особистим ключем подібне до підпису на паперовому документі. Але, на жаль, немає жодних гарантій, що, крім одержувача, повідомлення не прочитає будь-хто.

Використання криптографічних алгоритмів з відкритим ключем для шифрування повідомлень – достатньо повільний обчислювальний процес, тому фахівці-криптографи знайшли засіб швидко генерувати коротке унікальне подання особистого повідомлення, яке називається його дайджестом. Дайджест можна зашифрувати, а після цього використовувати особистий цифро-

вий підпис. Незважаючи на назву, дайджест повідомлення не є його стислим викладенням.

Існують поширені, швидкі криптографічні алгоритми для генерації дайджестів повідомлення – однобічні хеш-функції. Однобічна хеш-функція не використовує ключ. Це звичайна формула для перетворення повідомлення будь-якої довжини в один рядок символів – дайджест повідомлення. При використанні 16-байтової хеш-функції оброблений нею текст буде мати на виході довжину 16 байт, наприклад, повідомлення може бути надане ланцюжком символів VCC349RTYasdf904. Кожне повідомлення створює свій випадковий дайджест. Якщо зашифрувати дайджест особистим ключем, то утворюється цифровий підпис.

Наприклад, продавець А перетворив своє повідомлення в дайджест, зашифрував його своїм особистим ключем, і відправив В цей цифровий підпис разом з відкритим текстом повідомлення. Після того, як В використовує відкритий ключ А для розшифрування цифрового підпису, у нього буде копія дайджесту повідомлення А. Оскільки він зміг розшифрувати цифровий підпис відкритим ключем А, то А є його автором. Після цього В використовує ту ж саму хеш-функцію, про яку обидва домовилися заздалегідь, для підрахунку власного дайджесту для відкритого тексту повідомлення А. Якщо отриманий рядок співпадає з тим, що надіслав А, то В може бути впевнений в автентичності цифрового підпису. А це означає не тільки те, що відправник повідомлення – А, а також й те, що повідомлення не було змінене.

При такому підході єдина проблема полягає в тому, що повідомлення надсилається відкритим текстом, і, отже, його конфіденційність не зберігається. Для шифрування відкритого тексту повідомлення можна додатково використовувати симетричний алгоритм з секретним ключем. Але це призведе до подальшого ускладнення процесу.

Поки не існує бездоганної системи шифрування, яка цілком охоплює усі випадки захисту інформації. У таблиці 10 наводяться переваги і недоліки кожного різновиду шифрування.

Можна навести також порівняння витрат часу і грошей, необхідних для зламу ключів різної довжини (див. табл. 11).

Таблиця 10. Характеристика різних систем шифрування

Різновид шифрування	Переваги	Недоліки
1	2	3
Шифрування з симетричним ключем	Швидкість; легко реалізується апаратно	Обидва ключі однакові; важко розповсюджувати ключі; не підтримує цифрові підписи
Шифрування з відкритим ключем	Використовує два різних ключі; ключі розповсюджуються відносно легко; забезпечує цілісність і неможливість відмови від авторства за рахунок цифрового підпису	Працює повільно; потребує великих обчислювальних потужностей

Таким чином, усі вищезгадані способи не забезпечують абсолютного захисту інформації. Але вони:

- гарантують мінімально необхідний час для зламу від декількох місяців до декількох років. За цей час інформація, що передається, стає неактуальною;
- забезпечують, що вартість зламу на декілька порядків перевищує вартість самої інформації.

Таблиця 11. Порівняльна характеристика витрат часу і коштів для зламу ключів шифрування

Вартість, USD	Довжина ключа, біт				
	40	56	64	80	128
1	2	3	4	5	6

Продовження таблиці 11

1	2	3	4	5	6
100000	2 секунди	35 годин	1 рік	70000 років	1019 років
1000000	0,2 секунди	3,5 годи- ни	37 днів	7000 років	1018 років
100000000	2 мілісеку- нди	2 хви- лини	9 го- дин	70 ро- ків	1016 років
1000000000	0,2 мілісекун- ди	13 се- кунд	1 го- дина	7 років	1015 років
100000000000	0,2 мікресеку- нди	0,1 секу- нди	32 секун- ди	24 дні	1013 років

Однак спроби зламів ніколи не припиняються, завдяки й тому, що в мережі у вільному доступі весь час з'являються практично безкоштовні програмні засоби для порушення не дуже стійкого криптозахисту, й через застосування зловмисниками певних організаційних заходів.

Наприклад, зловмисники можуть розіслати усім абонентам Internet-провайдера електронного листа від імені системного адміністратора. У листі буде запропонована якась додаткова, звісно, безкоштовна послуга. Щоб передплатити її, користувачам слід надіслати листа з вказівкою свого логіна і пароллю. З декількох сотень чи тисяч клієнтів провайдера обов'язково знайдеться декілька не досить досвідчених користувачів, які відправлять дані, не звернувши уваги на те, що системному адміністратору зовсім не потрібно знати пароль користувача, і що електронна адреса, на яку вони відправляють листи, зовсім не адміністраторська. Таким чином, зловмисник водночас стає володарем декількох паролів. Щонайменша халепа, яка після цього очікує довірливих користувачів, – несанкціоноване використання їх облікових записів у провайдера.

Роль цифрових сертифікатів і сертифікаційних центрів.

Цифрові сертифікати слугують електронним підтвердженням відкритих ключів. Нагадаємо, щоб використовувати систему криптографії з відкритим ключем, необхідно згенерувати відкритий і особистий ключі. Зазвичай це робиться програмою, яка буде використовувати ключ: Web-браузером або програмою електронної пошти. Після того, як ключова пара згенерована, користувач має зберігати свій особистий ключ в таємниці від сторонніх. Після цього слід розповсюдити відкритий ключ серед своїх респондентів. Можна використовувати для цього електронну пошту, але такий підхід не забезпечує аутентифікації: хтось може згенерувати ключову пару і, приховуючись за іменем певного користувача, розіслати відкритий ключ респондентам. Після цього ніщо не завадить йому відправляти повідомлення від імені цього користувача.

Найкращий надійний шлях для розповсюдження відкритих ключів – користування послугами сертифікаційних центрів. Сертифікаційні центри несуть відповідальність за:

- перевірку особистості користувача;
- надання цифрових сертифікатів;
- перевірку їх справжності.

Сертифікаційний центр є сховищем цифрових сертифікатів. Цифрові сертифікати – електронний варіант посвідчення особистості і, ставши узвичасним засобом розповсюдження відкритих ключів, дозволяють респондентам користувача переконатися, що він – насправді той, за кого себе вдає. Центр приймає його відкритий ключ разом з доказами особистості, якими саме – залежить від класу сертифікату. Після цього респонденти користувача можуть звертатися до сертифікаційного центру за підтвердженням відкритого ключа користувача.

Відомі сертифікаційні центри, такі, як VeriSign, Cybertrust і Nortel, видають цифрові сертифікати, що містять: ім'я володаря, назву сертифікаційного центру, відкритий ключ для шифрування кореспонденції, термін дії сертифікату, зазвичай, від шести місяців до року, клас і ідентифікаційний номер цифрового сертифікату.

Виданий цифровий сертифікат може належати до одного з чотирьох класів, які вказують на ступінь верифікації володаря. Сертифікат першого класу отримати найлегше, оскільки тут вимагається мінімальна перевірка біографічних даних володаря, лише імені і адреси електронної пошти. При видачі сертифікату другого класу сертифікаційний центр перевіряє посвідчення особистості, номер картки соціального страхування і дату народження. Користувачі, які бажають отримати сертифікат третього класу, повинні бути готові до того, що додатково до інформації, необхідної для отримання сертифікату другого класу, сертифікаційний центр перевірить їх кредитоздатність, використовуючи спеціальні установи. Сертифікат четвертого класу додатково містить інформацію про посаду володаря в його установі, але відповідні верифікаційні вимоги тут ще не вироблені остаточно. Чим вище клас сертифікату, тим вище ступінь верифікації.

Щоб отримати цифровий сертифікат у комерційного або урядового сертифікаційного центру, користувач повинен внести певну плату, але є й виключення. Її розмір зростає з класом сертифікату, через додаткові зусилля, необхідні для перевірки особистих даних користувача. Завдяки точній перевірці даних біографії володарів сертифікатів вищих класів, останні можуть вважатися надійним підтвердженням особистості користувача. Сертифікаційні центри також несуть відповідальність за підтримку і публікацію списку недійсних сертифікатів.

Нині існують комерційні сертифікаційні центри, такі, як VeriSign, Cybertrust і Nortel, і державні, наприклад, Поштова служба США. Компанія може стати сертифікаційним центром і після цього видавати сертифікати своїм службовцям або іншим компаніям (див. рис. 27).

Всупереч думці про Internet, як про недостатньо надійний канал передачі інформації внаслідок його децентралізації, трансакції тут можуть бути добре захищені шляхом використання цього набору стандартів, охоплюючих захист усіх рівнів мережі – від пакету даних до програмного застосування (див. табл. 12). Стандарти забезпечують захист сполучень і програмних застосувань.

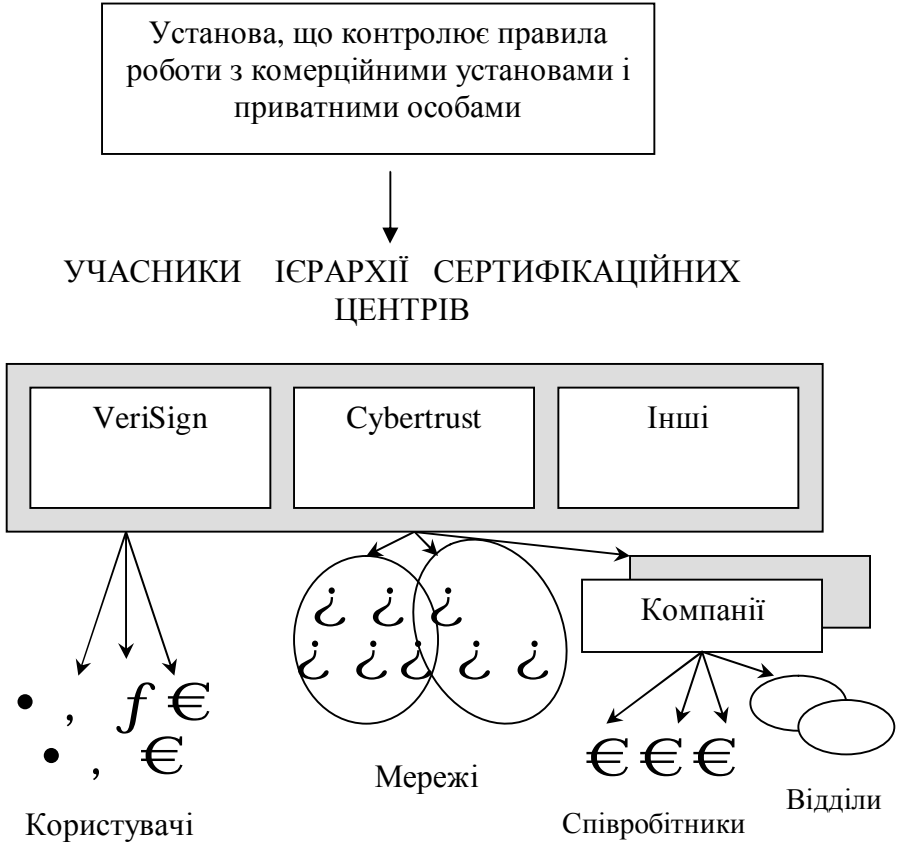


Рис. 27. Приклад ієрархії сертифікаційних центрів

Таблиця 12. Призначення стандартів для захисту усіх рівнів мережі

Стандарт (протокол)	Виконувана функція	Місце використання стандартів
1	2	3

Продовження таблиці 12

1	2	3
Secure HTTP (S-HTTP)	Захист трансакцій у Web	Програми-браузери, Web-сервери, програмні застосування для Internet
Secure Sockets Layer (SSL)	Захист пакетів даних на мережному рівні	Програми-браузери, Web-сервери, програмні застосування для Internet
Secure MIME (S/MIME)	Захист електронних повідомлень, які передаються за поштовим протоколом MIME	Поштові програми з підтримкою шифрування і цифрового підпису RSA
Secure Wide Area Network (S/WAN)	Шифрування одно-рангових сполучень між брандмауерами і маршрутизаторами	Віртуальні приватні мережі (VPN)
Secure Electronic Transaction (SET)	Захист трансакцій з кредитними картками	Смарт-картки, сервери трансакцій, електронна комерція

Web-застосування захищені двома протоколами – S-HTTP і SSL, які забезпечують аутентифікацію для Web-серверів і програм-браузерів, а також конфіденційність і цілісність даних для сполучень між сервером і браузером.

SSL – розробка компанії Netscape, що використовує криптографію з відкритим ключем, – механізм захисту інформації, який застосовується при роботі у WWW-системі. SSL можна використовувати не тільки для трансакцій, які здійснюються у Web, але цей протокол не призначений для забезпечення безпеки на основі аутентифікації, що відбувається на рівні програмного застосування або документа. Для управління доступом до

файлів і документів потрібно використовувати інші засоби. SSL оформився як офіційний стандарт захисту Web-серверів. Його підтримують домінуючі на ринкові програми-браузери компаній Microsoft і Netscape.

Для захисту електронної пошти в Internet існує безліч різноманітних протоколів, однак лише один чи два з них використовуються достатньо широко (S/MIME, PGP).

S/MIME – стандарт, в якому задіяно багато криптографічних алгоритмів, запатентованих і заліцензійованих компанією RSA Data Security Inc. S/MIME вживає цифрові сертифікати, і, отже, при забезпеченні аутентифікації спирається на використання сертифікаційного центру.

PGP – (Pretty Good Privacy, майже повна приватність) – родина програмних продуктів, які реалізують криптографію з відкритими ключами. Вона дозволяє як обмінюватися зашифрованими повідомленнями і файлами по каналах відкритого зв'язку без наявності захищеного каналу для обміну ключами, так і накладати на повідомлення і файли цифровий підпис. Програми родини PGP побудовані за принципом павутини довіри (Web of Trust) і дозволяють користувачам розповсюджувати свої ключі без посередництва сертифікаційних центрів.

Програма PGP була розроблена американським програмістом і громадянським активістом Філіпом Цимерманом, стурбованим порушенням особистих прав в інформаційну епоху. В 1991 р. у США існувала реальна загроза прийняття закону, який забороняв би використання стійких криптографічних засобів без так званого “чорного ходу”, використовуючи який спецслужби могли б переглядати зашифровані повідомлення. Тоді Цимерман почав безкоштовно розповсюджувати PGP в Internet. В результаті PGP став найпоширенішим криптографічним пакетом у світі (понад 2 млн. розповсюджених копій), а Цимерман зштовхнувся з трирічним переслідуванням влади за підозрою в незаконному експорті озброєнь.

Нині PGP розповсюджується на комерційних засадах заснованою Цимерманом фірмою PGP, Inc. PGP заборонена до експорту з США у вигляді програмного коду, що виконується, через це у решті світу використовуються міжнародні релізи програми, які обходять такі заборони.

Коли з'єднується ресурси корпоративної мережі установи, її сегменту чи окремого комп'ютера з відкритою мережею типу Internet, підвищується ризик атаків та пошкоджень як самих даних в мережі, так і комп'ютерної системи в цілому. Такий захист, як міжмережні екрани, або брандмауери, Firewall, добре служить для захисту даних і комп'ютерних систем. У вигляді програмного забезпечення, розташованого на комп'ютері з цінними для установи інформаційними ресурсами, або ж на окремому спеціалізованому комп'ютері чи пристрої міжмережні екрани призначені для захисту цих ресурсів або ресурсів усієї корпоративної мережі від користувачів з зовнішньої мережі.

Насамперед, міжмережні екрани працюють з програмами маршрутизації і фільтрами усіх мережних пакетів, щоб визначити, чи можна пропустити інформаційний пакет і, якщо можна, то відправити його до певної комп'ютерної служби за призначенням. Брандмауер є віртуальним кордоном, на якому перевіряється цілісність фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.

Налагодивши відповідним чином міжмережний екран, можна дозволити або ж заборонити користувачам як доступ із зовнішньої мережі до вузлів сегментів внутрішньої мережі, що захищається, так і доступ користувачів з внутрішньої мережі до відповідних ресурсів зовнішньої мережі.

Часто корпоративні мережі зв'язують офіси, розкидані містом, у регіоні, країні або ж у всьому світу. Провідні постачальники міжмережних екранів і маршрутизаторів запропонували технологію S/WAN (Secure Wide Area Networks). Вони взяли на себе впровадження і тестування протоколів, що пропонуються Робочою групою інженерів Internet (Internet Engineering Task Force, IETF) для захисту IP-пакетів. Ці протоколи забезпечують аутентифікацію і шифрування пакетів, а також засоби обміну і управління ключами для шифрування і аутентифікації. Протоколи S/WAN допоможуть досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників, що дозволить географічно віддаленим офісам однієї компанії, а також партнерам, що утворюють віртуальне підприємство, безпечно обмінюватися даними через Internet. Ця перспектива дозволить компаніям створювати свої власні віртуальні приватні мережі

(VPN) і використовувати Internet як альтернативу традиційним каналам зв'язку, які зазвичай орендуються за високу плату.

Однак, міжмережні екрани не є універсальним рішенням усіх проблем безпеки в Internet. Наприклад, вони не здійснюють перевірку на віруси і не здатні забезпечити цілісність даних.

Забезпечення захисту у платіжних системах Internet. Розглянуті вище технології захисту слугують основою для реалізації платіжних систем в Internet.

Як зазначалося, головне місце серед існуючих нині електронних платіжних систем посідають *системи з використанням кредитних карток*. Успіх застосування пластикових карток для розрахунків в Internet пов'язаний із звичністю такого типу оплати, подібного до оплати в реальному світі.

Описаний вище протокол SSL також в більшості випадків використовується для передачі інформації про пластикові картки. Однак цей засіб має деякі недоліки. Хоча перехопити інформацію під час транзакції практично неможливо, важлива інформація у випадку несумлінного її зберігання на сервері продавця може знаходитися під загрозою доступу до неї зловмисників. До того ж існує можливість підробки або підміни справжності торговця або особистості користувача як продавцем, так і покупцем. Фірма може надати про себе невірну інформацію, а покупець – зробити замовлення, а після відмовитися від оплати. Довести, що саме він користувався своєю картою, практично неможливо через відсутність підпису.

Технологією, закликаної усунути ці недоліки, є вищезгаданий протокол SET. Він розроблений компаніями MasterCard і Visa при підтримці Netscape, IBM, VeriSign тощо і базується на криптографії з використанням публічних ключів і цифрових сертифікатів. У відповідності з технологією SET номер картки, що передається мережею, шифрується з використанням електронного підпису клієнта. Дешифрування можуть здійснювати тільки уповноважені банки і компанії, здійснюючі обробку транзакцій за картками.

Протокол SET має забезпечити захист клієнтів від несумлінних продавців і захист продавців від шахрайства шляхом використання підроблених або викрадених карток. Недоліком SET сьогодні є те, що користувачам цієї технології слід встановлю-

вати у себе відповідне програмне забезпечення, що вимагає значних інвестицій. Крім того, висловлюються думки про недостатню високу швидкість проведення трансакцій.

Найперспективнішими формами електронних платежів з точки зору їх захищеності є використання *смарт-карток й іншої цифрової готівки*. Готівкові цифрові гроші на основі смарт-карток можуть не тільки забезпечити необхідний рівень конфіденційності і анонімності, але і не вимагають зв'язку з центром для підтвердження оплати. У зв'язку з цим вартість трансакції може бути зведена нанівець.

Перераховані властивості смарт-карток дозволяють прогнозувати поступове розповсюдження цього різновиду платіжних систем в Internet. Однак для їх застосування в якості засобу оплати в мережі Internet вимагається широке розповсюдження відповідних периферійних приладів для персональних комп'ютерів, призначених для зчитування даних зі смарт-карток.

Надійну роботу систем з використанням цифрової готівки забезпечують сучасні засоби криптографії: алгоритми криптографії з відкритим ключем, електронного підпису і електронного "сліпого" підпису. Витрати на функціонування таких систем мінімальні. До того ж, відсутність у схемах розрахунків кредитної картки, а звідси – і значних витрат на оплату трансакцій процесінговим компаніям, дозволяє застосовувати їх для мікроплатежів, тобто розрахунків в самому нижньому ціновому діапазоні, менше одного долару.

За загальною думкою, саме мікроплатежі здатні обслуговувати основний обсяг продажів інформації в Internet. До того, цифрова готівка може забезпечити повну анонімність, бо не містить жодної інформації про клієнта, який їх витратив. Серед світових компаній, які розвивають системи цифрової готівки, слід згадати NetCash, CyberCash, DigiCash, Mondex, в Україні і Росії – PayCash, WebMoney Transfer.

Порівняльний аналіз розповсюджених в Uanet і Runet платіжних електронних систем точки зору їх рівня безпеки і конфіденційності наведений у таблиці 13.

Через те, що електронні гроші і смарт-картки поки не отримали широкого розповсюдження в Україні і Росії, найбільш реальними для вітчизняного мережного споживача залишаються

Таблиця 13. Порівняльний аналіз безпеки електронних платежів з використанням різних платіжних Internet-систем

Платіжна Internet-система	Рівень безпеки	Конфіденційність
WebMoney Transfer	Уся інформація, яка передається по каналах Internet, закодована із стійкістю не менш, ніж RSA з довжиною ключа у 1040 біт	Цілком анонімна система для покупця і продавця
CyberPlat	Система використовує асиметричний алгоритм криптографічного перетворення (ключ у 512 біт)	Для покупця система неанонімна
PayCash	Система використовує шифрування з відкритим (RSA з ключем у 1024 біт) і закритим ключами (ключ у 160 біт)	Цілком анонімна система для покупця: ані банк, ані продавець не можуть визначити покупця. Продавець банком не визначається

платежі пластиковими картками. При цьому забезпечується достатньо високий ступінь захисту інформації як покупця, так і продавця. Проблемами залишається те, що, по-перше, національні банківські системи країн СНД поки не готові до широкого використання карток, електронної готівки як засобів електронних платежів; по-друге, наші користувачі не схильні, а часто й не здатні, передавати через Internet конфіденційну інформацію через низьку інформаційну культуру.

Нині навіть у розвинених інформаційних суспільствах спостерігається певний парадокс: якщо сучасні програмні засоби захисту інформації, що передається через мережу, дозволяють як ідентифікувати користувача, так і забезпечити достатній рі-

вень безпеки даних, юридична база електронної комерції поки не відповідає рівню розвитку технологій захисту інформації через бідну практику використання і носить часто декларативний характер.

3.2.3. Служби доставки

Усі кур'єрські служби, як фірми, що спеціалізуються на логістиці, тобто доставці кореспонденції й вантажів адресату, готові співпрацювати з електронними крамницями, розуміючи, що електронна комерція має величезний потенціал для розвитку ринку послуг доставки.

Донещодавна більша кількість західних Internet-крамниць мала власний штат кур'єрів або власну кур'єрську службу. Електронні крамниці зверталися до послуг служб експрес-перевезення тільки тоді, коли товар слід було доставити в регіони. Але останнім часом крамниці все активніше звертаються до послуг незалежних служб доставки. Утворюються нові компанії, зорієнтовані на обслуговування Internet-економіки; відомі компанії розробляють й впроваджують рішення для електронної комерції.

Втчизняні служби експрес-доставки, що не мають спеціальної ліцензії на інкасацію, можуть доставляти тільки ті товари, які споживач оплатив заздалегідь кредитною карткою або за перерахуванням, тоді, як клієнти схильні оплачувати покупку безпосередньо кур'єру. На Заході такої проблеми практично не існує.

Нині на ринкові діють різноманітні компанії, що надають кур'єрські послуги: транснаціональні компанії експрес-доставки, так звана "велика четвірка" (DHL, TNT, UPS, FedEx); національні оператори європейських компаній; національні українські компанії; невеликі компанії, що доставляють кореспонденцію виключно у межах Києва й області. Ціни на послуги цих компаній розрізняються в 3-5 разів й залежать від терміна доставки, об'єма замовлення й ваги вантажу. Постійним клієнтам зазвичай надаються знижки.

В залежності від специфіки певні національні компанії здійснюють доставку лише у визначені міста, інші готові доставити її в будь-який населений пункт України. Подібна ситуація й в Росії. Крім експрес-доставки за принципом "від двері до двері", більшість кур'єрських служб надає більш економічні послуги: від двері замовника до міста призначення або ж доставка кореспонденції чи вантажу літаком до великого європейського міста, де вона опиняється у поштовій скриньці і далі доставляється вже європейською поштовою службою.

Кур'єрські служби зазвичай пропонують й додаткові послуги: страхування, митне оформлення й складування вантажів, комплексні логістичні рішення, надання інформації про місцезнаходження вантажу. Невеликі національні компанії часто мають власні бази даних і здійснюють адресні розсилання інформаційних і рекламних матеріалів замовника.

Представник "великої четвірки" – компанія DHL (www.dhl.com) – працює у 228 країнах світу й першою запропонувала надання послуг з міжнародної експрес-доставки на території ще тоді Радянського Союзу. Транспортна система DHL має 33 міжнародних сортувальних центри, власний повітряний флот з 252 літаків й автомобільний парк з 18 тисяч одиниць. В компанії працює 64 тисячі співробітників. Компанія надає послуги в галузі електронної комерції й співпрацює з українськими і російськими електронними крамницями. На сайті компанії можна оформити замовлення на виклик кур'єра, отримати інформацію про місцезнаходження й статус відправлення, розрахувати об'ємну вагу вантажу й отримати повний набір митної документації.

Компанія TNT з цієї ж групи кур'єрських служб (www.tnt.com) надає послуги з термінової доставки документів, вантажів усіх різновидів практично в будь-яку країну світу і є одним з визнаних європейських лідерів на ринкові експрес-доставки. В TNT працює понад 50 тис. чоловік. Вона володіє власним автомобільним парком з 17215 одиниць й повітряним флотом з 60 літаків, здійснюючи 3,2 млн. відправлень кожного тижня.

Минулого року компанія оголосила про початок роботи на території Росії інтегрованої системи електронної торгівлі TNT

Loop. TNT Loop передбачає контроль з єдиного центра за усім комплексом заходів із забезпечення процесу електронної торгівлі: прийомом замовлень, оплатою, складуванням й зберіганням товарів, транспортуванням й доставкою замовлень, післяпродажним обслуговуванням. Нині ця система запроваджена в електронній крамниці компанії Sony.

Причини, з яких фірмам, зайнятим електронною комерцією варто скористатися послугами логістичного підприємства з перевезення й експедиванню товару такі:

- це дозволяє не утримувати свій штат диспетчерів й логістиків з перевезень;
- відправлення товарів кінцевим споживачам можна організувати з мінімальними витратами;
- логістичне підприємство надає гарантії якісної доставки і матеріальної відповідальності за вантаж, що перевозиться.

В Україні на ринку послуг логістики діє ГППС “Укрпочта” й приватні кур’єрські служби типу “Офіс-Сервіс”.

3.2.4. Реклама і маркетинг в глобальній мережі

Проведення реклами в Internet. Важливим механізмом підтримки ефективної електронної комерції є Internet-реклама. В опублікованому в серпні 1999 року другому виданні відомої книги Р. Зефа і Б. Аронсона "Реклама в Internet" наводиться два її визначення:

- “Internet-реклама – конвергенція традиційної реклами і маркетингу прямого відгуку (direct response marketing)”;
- “Internet-реклама – це конвергенція брендинга, розповсюдження інформації і продажів – усе в одному місці (С. Кінан, віцепрезидент компанії America Online)” [18].

Internet-реклама має наступні переваги у порівнянні з її традиційними формами:

- вона відносно дешева, адже витрати на виробництво мережних газет і журналів в декілька раз нижче, ніж друкованих ЗМІ, не кажучи вже про телебачення і радіомовлення;
- легко перетинає кордони. Якщо вдало розташувати Web-сайт фірми й інформацію про нього, про компанію та її товари і послуги дізнаються в усьому світі;
- має високий рівень спеціалізованості. Найбільш ефективною вважається реклама в спеціалізованих виданнях. Сайти також можна вважати такими: вони присвячені певній тематиці, а користувачі зазвичай відвідують сайти відповідно до своїх інтересів, де на них і чекає реклама.

Перша реклама в Internet з'явилася у 1994 році у спеціалізованих комп'ютерних журналах типу Hot Wired. Предметом реклами насамперед були комп'ютерні технології, через обмеженість і специфічність кола користувачів Internet на початку 1990-х років. Серед перших рекламодавців такої реклами були корпорації AT&T і IBM.

Рекламні модулі в Internet – банери – відзначаються своєрідною природою, схожею на пасткову: натиснувши на них мишею, можна влучити на сайт компанії-рекламодавця, з якого інколи вдається повернутися назад, натискуючи піктограму Back (Назад) на панелі інструментів програми-браузера. Однак, в деяких банерних проєктах цього зробити не можна (див. рис. 28). Такого не можна реалізувати ані в друкованих ЗМІ, ані на радіо і телебаченні.

За оцінками експертів, останнім часом найбільш дієвими є рекламні модулі категорії rich media, здатні пересуватися Web-сторінками, а також засоби показу віртуальної реклами, створені за технологією MacroMedia Flash [6]. Подібні рекламні модулі нині складають 37% ринку Web-реклами. Поширеність подібної реклами пов'язана з високим коефіцієнтом ефективності: головний чинник, за яким визначається цінність мережної реклами – CTR (click through rates) – нині у п'ять разів вище, ніж у традиційних форматів у 468x60 пікселів й вертикального розміщення. CTR визначається як співвідношення числа відвідувань сайту і кількості банерних показів.

Розцінки на будь-яку рекламу пов'язані в більшості випадків з розмірами аудиторії. В друкованих ЗМІ це вимірюється тиражем, на телебаченні і радіо – передбачуваною кількістю глядачів і слухачів.



Рис. 28. Різновиди банерів стандартних форматів

В мережних виданнях плата за рекламу залежить від кількості хітів (людино-відвідувань). Якщо тираж газети не розпродався, то рекламодавець залишається в програвші, бо його інформація не потрапила до тієї кількості людей, на яку він розраховував. В Internet реклама може знаходитися на Web-сайті доти, доки його не відвідають потрібну кількість разів. Як на радіо і телебаченні, в Internet-рекламі можна стягати плату за найбільш "гарячий" час у проміжках між 12.00-16.00 і 19.00-23.00 годинами. У банерообмінних мережах – специфічно інтернетовському

явищі – існує обмін банерами між Web-сайтами – членами мереж, який діє за принципом “Ми рекламуємо Вас, Ви – нас”.

Фірми, вочевидь, завжди зацікавлені в оцінці ефективності використання ними маркетингових і рекламних можливостей Internet. Найголовніше в певній кампанії оцінювати те, що було її маркетинговою метою. Якщо це – просування торгової марки, то не має сенсу підраховувати, скільки людей прийшло за певним гіперпосиланням на сайт фірми з того чи іншого банеру. Значно більш цікаво те, скільки разів він був показаний, тобто скільки людей мали шанс запам'ятати торгову марку фірми.

Один з можливих способів оцінити реальну ефективність маркетингової кампанії фірми – двічі провести опитування користувачів її корпоративного сайту: перший раз, розташувавши там торгову марку, що рекламується, перед початком рекламної кампанії і другий – після її завершення. Порівняння статистики щодо поширеності цієї торгової марки і охарактеризує ефективність результату.

Якщо метою рекламної кампанії було проведення розпродажу, реальна оцінка її ефективності може розраховуватися як співвідношення кількості приходів користувачів до корпоративного сайту чи Internet-крамниці з певного банеру до кількості його показів аудиторії, зацікавленої в запропонованих товарах, а не просто до загальної кількості його показів. Відсоток відвідувачів сайту фірми чи Internet-крамниці, зацікавлених в таких товарах, можна оцінити за результатами заздалегідь проведеного простого опитування.

Більш детально питання ефективності систем електронної комерції й дії її підтримуючого механізму – мережної реклами – розглядаються у розділі 4.

Internet-маркетинг. Було б цілком невірним ідентифікувати маркетингові можливості мережі з проведенням в ній тільки реклами. Internet як потужний маркетинговий канал характеризується безсумнівними перевагами перед іншими медіа, а саме:

§ таргетингом – точним охопленням цільової аудиторії: географічним, за часом, за тематичними сайтами;

§ трекінгом – можливістю аналізу поведінки відвідувачів корпоративного сайту і вдосконалення як самого сайту, так і проду-

кції і послуг, системи маркетингу фірми у відповідності з висновками такого аналізу;

§ доступністю за принципом 24/24 і 7/7: 24 години на добу, 7 днів на тиждень і гнучкістю: почати, скоригувати і перервати рекламну Internet-кампанію можна миттєво;

§ інтерактивністю: споживач може взаємодіяти з продавцем і з продуктом, вивчати його, інколи апробувати, наприклад, ознайомитися з демо-версією програми, переглянути розділ книги в Internet-крамниці тощо, і, якщо товар влаштовує, придбати його;

§ можливістю розміщення великої кількості рекламної інформації, включаючи графіку, звук, відео- та інше;

§ оперативністю розповсюдження і отримання інформації;

§ порівняно низькою вартістю рекламних послуг;

§ можливістю більш пильної уваги користувача перед комп'ютером, концентрації на деталях;

§ можливістю створення віртуальних спілок споживачів (on-line community) за інтересами, професійними заняттями, тобто цільової аудиторії.

Вже йшлося про те, що для компанії доцільно мати власний корпоративний Web-сайт з брендовим ім'ям, унікальним дизайном, наочним і привабливим поданням фірми та її пропозицій, можливо і у вигляді Internet-крамниці. Після створення сайту слід зробити його відомим цільовій аудиторії.

Основні засоби Internet-маркетингу, з допомогою яких можна вирішувати це завдання:

§ розміщення (індексування) сайту у відомих пошукових системах, каталогах і рейтингах, таких, як західні Yahoo!, AltaVista, Exite, HotBot, Lycos, українські Meta, InfoRes, російські Яндекс, Rambler, Апорт;

§ реклама на тематичних сайтах і тих, які найчастіше відвідуються;

§ контекстна реклама. Наприклад, Internet-крамниця Amazon.com встановила виключні партнерські стосунки з Yahoo! щодо контекстних рекламних об'яв;

§ участь в банерообмінних мережах;

§ обмін між серверами кнопками, банерами, посиланнями. Так, керівництво Amazon.com за публікацію посилань, які сприяють

збільшенню її обсягів продажів, виплачує комісійні більш, ніж 100 тис. Web-вузлів.

Фірмам доцільно розташовувати інформацію про себе і позиції в он-лайнових каталогах, на електронних дошках оголошень, в електронних прайс-листах і базах даних, на сайтах, які висвітлюють тематичні новини, у форумах, а також надавати інформацію зацікавленим електронним виданням і проектам. Internet можна активно використовувати для просування пропозицій компанії, маючи навіть тільки E-mail. Тут використовуються такі засоби, як:

§ direct-mail – спрямована розсилка рекламних листів за певним колом електронних адрес, яка, однак, не переходить до форми спаму;

§ телеконференції.

При цьому користувачам E-mail відкриваються можливості отримання інформації, наприклад, через передплату на списки розсилки, новини серверів. Однак, чим вище рівень використання Internet у фірми, тим більше у неї маркетингових можливостей у мережі.

Прикладом різноманітних маркетингових можливостей Internet для фірми є Туристичний інформаційний сервер (www.tour.com.ua). На ньому розміщений "Каталог Тур-WWW України", до якого турфірми можуть вносити посилання на свої фірмові сайти. Певні пропозиції турфірми можуть подати в "Базі пропозицій турфірм", яка має пошукові засоби, що зручно для користувача. Щотижня на сайті виходить розсилка туристичних новин, в яку турфірми можуть відправити новини про свою компанію або просто цікаву новину, а вказівка на респондента – це реклама фірмі. На сайті практикуються рекламні банери і кнопки на окремих або на всіх Web-сторінках, текстова і банерна реклама в розсилці, Web-сторінки в каталозі турфірм (електронні візитні картки), що дозволяє стороннім фірмам мати своє представництво в Internet при мінімальних фінансових витратах. Корисну і цікаву для відвідувачів сайту – потенційних клієнтів інформацію – можна розташувати за підписом певної туристичної фірми в різних розділах сайту і таким чином сприяти її позитивному іміджу. Вищезазначений туристичний сайт – найбільш

відвідуваний в Україні за цим напрямком, тому реклама на ньому є надзвичайно ефективною для туристичних фірм.

Однак, з часом Internet скасує потребу споживачів у послугах туристичних фірм, як класичних посередників, бо через мережу можна замовити й номери в готелях в країні відпочинку чи ділової поїздки, й квитки на літак або потяг тощо.

Подібні приклади використання багатих можливостей Internet-маркетингу можна було б навести для компаній будь-якої сфери бізнесу.

Останнім часом важливим питанням для керівництва будь-якої фірми є адекватність витрат на інформаційно-комунікаційні технології вартісним результатним показникам її роботи. Як вказувалося, прямий кореляційний зв'язок між цими чинниками спостерігається лише у компаній інформаційного сектору. Для фірм традиційних галузей цей вплив опосередований й не визначається лише у вартісній формі. Проблематиці визначення економічної ефективності інформаційних систем компаній, в першу чергу систем, присвячений матеріал наступного розділу.

Література

1. Закон України “Про захист інформації в автоматизованих системах”./ Відомості Верховної Ради. – 1994. – №31. – с. 286.
2. Макарова М.В. Електронна комерція. Посібник. – К.: Видавничий центр «Академія», 2002. – 272 с.
3. Пономаренко Л.А., Филатов В.О. Електронна комерція. Підручник / За ред. Мазаракі А.А. – К.: Київ. Нац.торг.-екон. ун-т, 2002.– 443 с.
4. Козье Д. Электронная коммерция. – М.: Русская редакция, 1999. – 288 с.
5. Шарма В., Шарма Р. Разработка Web-серверов для электронной коммерции (Комплексный подход). Учебное пособие. – М.: Издательский дом “Вильямс”, 2001. – 400 с.

6. Будущее сетевой рекламы.// Компьютер-ИНФО. – 2003. – № 21 (330). – http://www.cinfo.ru/CI/CI_330_21/Articles/Reclama_330.htm.
7. Положення про порядок здійснення криптографічного захисту інформації в Україні. Затверджено Указом Президента України від 22 травня 1998 року №505.98. – <http://www.ipc.kiev.ua/ukr/laws.asp.?type=article&num=180>.
8. Багрин Ю. Internet – новые инструменты в маркетинговой деятельности предприятий. // В сборнике тезисов докладов конференции “Internet-комерція-2000”. – К.: 2000. – <http://www.ecworld.com.ua:8001/ic99/bagrин.html>.
9. Бойчун О.В. Технология коммерческих и денежных операций в Internet. // В сборнике тезисов докладов конференции "Internet-комерція-2000" – К.: 2000. – <http://www.ecworld.com.ua:8101/ic99/e-comm.html>.
10. Волков С. Система электронных платежей PayCash. // В сборнике тезисов докладов на семинаре “Электронная коммерция – путь успешного бизнеса в России”. – М.: 2000. – <http://www.magazin.ru/tez.html>.
11. Кузнецов В. B2C: состояние и перспективы.// В сборнике материалов конференции "Перспективы использования интернет-технологий в бизнесе". – Ярославль: 2003. – http://www.e-commerce.ru/analytics/statistics/b2c_state.html.
12. Багрин Ю. Интернет как новый маркетинговый канал.// Журнал “Маркетинг и реклама”. – 1999. – №11. – <http://www.i-m.kiev.ua/publ/1.htm>.
13. Волков С., Достов В. Платежные механизмы современного Internet. // Журнал “Мир Internet”. – 2000. – №5. – с. 22–28.
14. Калачник В. Директ Маркетинг в Украине: Состояние и перспективы. // REX Navigator. – 2002. – №9. – <http://osdirect.com.ua/publish/46/>
15. Мурадян А. ИТ-бюджет – приятного аппетита! // Business Online. – 2001. – № 4. – с. 53-56.
16. Уолш Б. Протоколы для платежей через Интернет. – http://www.ccc.ru/magazine/depot/99_09/print.html?77.

17. Морейнис А. Четыре источника и четыре составных части Интернет-маркетинга. – <http://www.marketer.ru/articles/index.73.html>.
18. Zeff R., Aronson B. Advertising on the Internet: 2-nd edition. – 1999.