УДК 004.413.4, 004.942, 007.5, 65.011.3, 681.518

А.Ю. Берко, В.А. Висоцька, І.В. Рішняк
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Проаналізовано основні методи та засоби оцінювання ризиків систем захисту інформації у сфері електронного бізнесу та шляхи зменшення рівня цих ризиків.

The analysis of basic methods and facilities of evaluation of risks of the systems of priv in the field of electronic business and ways of diminishing of level of these risks is conducted in the article.

Вступ

Під інформаційною безпекою (ІБ) системи електронної комерції (СЕК) розуміють захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних нанести збитки власникам або користувачам інформації. Будь-яке порушення безпеки інформації в електронній комерції може бути розглянуте в термінах загроз, уразливості та атак [1].

Загальна постановка проблеми та її зв'язок із важливими науковими та практичними завданнями

З положення про безпеку інформації в електронній комерції можна зробити два важливі висновки [14]:

§ Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно відрізнятися, наприклад, безпека для закритих державних організацій та комерційних структур;

§ Інформаційна безпека не полягає винятково у захисті інформації. Це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (отримати матеріальні і/або моральні збитки) не тільки від несанкціонованого доступу до інформації, але і від пошкодження системи, що зумовить перерву в роботі. Для багатьох відкритих організацій (наприклад, навчальних) захист інформації не є першочерговою задачею.

Проблеми безпеки інформації. У теорії інформаційної безпеки існує основна теорема безпеки системи, яка доведена для багатьох типів математичних моделей захищених систем і формулюється так: "***Якщо початковий стан системи безпечний і всі переходи системи із стану в стан безпечні, то система безпечна***". Абсолютно очевидно, що для безпечно захищеної СЕК умови даної теореми повинні підтримуватися на всіх стадіях життєвого циклу системи. При цьому основна теорема безпеки системи трансформується в основну теорему безпеки для програмного забезпечення системи: "***Якщо програмне забезпечення системи починає свої операції в безпечному стані і всі переходи системи із стану в стан безпечні, то всі стани системи безпечні***".

Серед основних вимог до проведення комерційних операцій – конфіденційність, цілісність, аутентифікація, авторизація, гарантії та збереження таємниці [1–4, 16–17]. Перші чотири вимоги забезпечуються технічними та програмними засобами, але виконання останніх двох – досягнення гарантій і збереження таємниці – однаково залежить як від програмно-технічних засобів та відповідальності окремих осіб і організацій, так і від дотримання законів, що захищають споживача від можливого шахрайства. У реальному світі ми багато уваги приділяємо фізичній безпеці, а у світі

електронної комерції доводиться піклуватися про засоби захисту даних, комунікацій і транзакцій. Маючи справу з мережевими системами Internet та Intranet, треба пам'ятати про існування декількох можливих загроз:

- Дані навмисно перехоплюються, читаються чи змінюються;
- Користувачі навмисно ідентифікують себе неправильно;
- Користувач одержує несанкціонований доступ з однієї мережі до іншої.

Вказані загрози реалізуються через такі уразливі місця:

1. **Уразливості сервісів TCP/IP** – ряд сервісів TCP/IP є небезпечними і можуть бути скомпрометовані розумними зловмисниками. Особливо вразливі сервіси, що використовуються в локальних обчислювальних мережах (ЛОМ) для поліпшення управління мережею;
2. **Легкість спостереження за каналами та перехоплення інформації** – більшість трафіку Інтернет не зашифровано. Електронна пошта, паролі та файли, що передаються, можуть бути перехоплені при використанні легкодоступних програм. Потім зловмисники можуть використати паролі для проникнення в системи електронної комерції;
3. **Відсутність політики** – багато мереж можуть бути сконфігуровані через незнання так, що даватимуть можливість доступу до них з Інтернету, не враховуючи можливих зловживань. Значна кількість мереж допускає використання більшої кількості сервісів TCP/IP, ніж це потрібно для діяльності їх організації. Адміністратори таких мереж не намагаються обмежити доступ до інформації з комп'ютерів. Це може допомогти зловмисникам проникнути до мережі;
4. **Складність конфігурування** – ресурси управління доступом до мереж у хостах часто є складними в налаштуванні та контролі за ними. Неправильно сконфігуровані засоби часто призводять до неавторизованого доступу;
5. **Помилки при конфігуруванні хоста або ресурсів управління доступом**, які або погано встановлені, або настільки складні, що важко адмініструються;
6. **Роль та важливість адміністрування системи**, які часто не враховуються під час опису посадових обов'язків співробітників (більшість адміністраторів наймаються на неповний робочий день є низькокваліфікованими);
7. **Слабка аутентифікація**;
8. **Можливість легкого спостереження за даними, що передаються**;
9. **Можливість легкого маскування під інших**;
10. **Недоліки служб ЛОМ та взаємної довіри хостів один до одного**;
11. **Складність конфігурування і заходів захисту**;
12. **Слабкий захист на рівні хостів**.

У забезпеченні інформаційної безпеки в електронній комерції зацікавленими є три різні категорії суб'єктів: державні організації, комерційні структури та окремі громадяни.

Аналіз сучасних досліджень і публікацій та виділення проблем

Заходи забезпечення безпеки інформації. Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати заходи таких рівнів:

- законодавчого (закони, нормативні акти, стандарти тощо);
- адміністративного (дії загального характеру організації, які виконуються керівництвом);
- процедурного (конкретні заходи безпеки, що мають справу з людьми);
- програмно-технічного (конкретні технічні заходи).

Законодавчий рівень. Законодавчий рівень є найважливішим для забезпечення ІБ СЕК. До цього рівня ми зараховуємо весь комплекс заходів, спрямованих на створення і підтримку в суспільстві негативного (зокрема відповідальності і покарань) відношення до порушень і порушників ІБ СЕК [1]. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і/або карається суспільством, тому що так діяти не прийнято. Найважливішим на законодавчому рівні є створення механізму, що дає змогу узгодити процес розроблення законів з прогресом інформаційних технологій. Природно, закони не можуть

випереджати життя, але важливо, щоб відставання не було надто великим, оскільки на практиці це призводить до зменшення рівня ІБ.

Адміністративний рівень. Основою заходів адміністративного рівня, тобто заходів, що розробляються керівництвом організації, є політика безпеки при електронній комерції [2]. Під такою політикою безпеки розуміють сукупність документованих управлінських рішень, спрямованих на захист інформації і асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в галузі інформаційної безпеки, а також ту міру уваги і кількість ресурсів, які керівництво вважає доцільним виділити. Вона будується на основі **аналізу ризиків**, які є реальними для системи електронної комерції організації. Коли ризики проаналізовані і стратегія захисту визначена, складається програма, реалізація якої повинна забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні особи, встановлюється порядок контролю виконання програми і т.п. Розробка політики безпеки – справа тонка, оскільки кожна організація має свою специфіку. Безглуздим є застосовування практики закритих державних організацій на комерційні структури. У цій сфері доцільно використовувати основні принципи розроблення політики безпеки та готові шаблони для найважливіших типів організацій.

Процедурний рівень. До процедурного рівня належать заходи безпеки, що реалізуються людьми. У вітчизняних організаціях накопичений багатий досвід складання і здійснення процедурних (організаційних) заходів, однак проблема полягає в тому, що вони прийшли з докомп'ютерного минулого і тому потребують істотного перегляду.

Можна виділити такі групи процедурних заходів:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

Для кожної групи в кожній організації повинен існувати набір регламентів, які визначають дії персоналу. Своєю чергою, виконання цих регламентів потрібно відпрацьовувати на практиці.

Програмно-технічний рівень. Згідно із сучасними переконаннями, у межах систем електронної комерції повинні існувати принаймні такі механізми безпеки [17]:

- ідентифікація й перевірка автентичності користувачів;
- управління доступом;
- протоколювання та аудит;
- криптографія;
- екранування;
- забезпечення високої продуктивності.

Спектр інтересів суб'єктів, пов'язаних з використанням СЕК, можна поділити на такі основні категорії:

- конфіденційність (захист від несанкціонованого ознайомлення);
- цілісність (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);
- доступність (можливість за прийнятний час одержати необхідну інформаційну послугу).

Конфіденційність. Цей аспект ІБ найбільш відпрацьований у нашій країні. На варті конфіденційності стоять закони, нормативні акти, багаторічний досвід відповідних служб. Вітчизняні апаратно-програмні продукти дають змогу закрити практично всі потенційні канали відтоку інформації.

Цілісність. Її можна поділити на статичну (зрозумілу як незмінність інформаційних об'єктів) і динамічну (що стосується конкретного виконання складних дій (транзакцій)) [1]. Практично всі нормативні документи і вітчизняні розробки належать до статичної цілісності, хоча динамічний аспект не менш важливий. Приклад динамічної цілісності – контроль потоку фінансових повідомлень (виявлення крадіжки, упорядкування або дублювання окремих повідомлень).

Доступність. Системи електронної комерції створюються для отримання певних інформаційних послуг (сервісів). Якщо за тих або інших причин отримання цих послуг користувачами стає неможливим, це, очевидно, наносить збиток усім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим аспектам, ми виділяємо її як найважливіший елемент інформаційної безпеки [1–4]. Особливо яскраво провідна роль доступності проявляється у таких системах електронної комерції, як:

§ системи підтримки електронної взаємодії різних служб при підготовці авіаційних, залізничних і автомобільних рейсів;

§ торгові системи, які призначені для організації Інтернет-торгівлі і реалізують стосунки типу „продавець–покупець"; системи „бізнес–бізнес", де реалізована схема повністю автоматизованої взаємодії бізнес-процесів між двома організаціями. Це можуть бути аукціони; фінансові, банківські, туристичні, медичні, страхові, інформаційні послуги; онлайнова оплата рахунків тощо.

Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей: продаж залізничних та авіаквитків, банківські послуги тощо.

Отже, інформаційна безпека повинна забезпечувати: конфіденційність інформації, цілісність даних – захист від збоїв, що ведуть до втрати інформації та неавторизованого створення або знищення даних, а також доступність інформації для всіх авторизованих користувачів.

Для всіх функцій і задач СЕК повинні бути дані відповідні визначення. Потім визначають механізми безпеки, які реалізують ці функції. Основні механізми інформаційної безпеки такі:

§ управління доступом до інформації;
§ ідентифікація та аутентифікація;
§ криптографія;
§ екранування;
§ забезпечення цілісності і доступності даних;
§ підтримка працездатності системи електронної комерції при збоях, аваріях, НС;
§ відстеження подій, які можуть загрожувати ІБ;
§ управління доступом у системах електронної комерції;
§ протоколювання дій і подій.

Якщо використовується опис вимог за підсистемами, повинні бути сформульовані додаткові вимоги, регламентовані у вимогах вибраного профілю захисту (класу захищеності системи електронної комерції від несанкціонованого доступу). Можливе використання змішаного підходу, за якого додаткові вимоги описуються в термінах функцій (сервісів) безпеки. Однак з метою вивчення безпеки в електронній комерції сьогодні можна виділити чотири класи обміну даними в мережах для електронної комерції: електронна пошта, електронний обмін даними, інформаційні транзакції, фінансові транзакції [7–8].

Основні складові безпеки систем електронної комерції

Електронна пошта є дешевим засобом взаємодії з клієнтами, діловими партнерами і з її використанням пов'язаний ряд проблем з безпекою:

§ адреси електронної пошти в Інтернет легко підробити;

§ електронні листи можуть бути просто модифіковані. Стандартний SMTP-лист не містить ресурсів перевірки їх цілісності;

§ електронну пошту можуть прочитати на кожній проміжній робочій станції;

§ немає гарантій доставки електронного листа. Хоч деякі поштові системи надають можливість отримати повідомлення про доставку, часто такі повідомлення означають лише те, що поштовий сервер одержувача (а не обов'язково сам користувач) отримав повідомлення.

Електронний обмін даними (EDI). Найпростіша форма – це обмін інформацією між двома бізнес-суб'єктами (торговими партнерами) у стандартизованому форматі. Базовою одиницею обміну є набір транзакцій, який загалом відповідає стандартному бізнес-документу, такому як

платіжне доручення або накладна на товар. За допомогою стандартів, основу яких становлять X.9 і UN/EDIFACT, ділове співтовариство розробило групу стандартних наборів транзакцій [11].

Кожний набір транзакцій складається з великої кількості елементів даних, необхідних для даного бізнес-документа, кожний з яких має свій формат і місце серед інших елементів даних. Компанії почали використовувати EDI, щоб зменшити час і витрати на контакти з постачальниками. Так, в автомобільній промисловості великі компанії вимагали від постачальників використати EDI для всіх транзакцій, що дозволило зберегти безліч паперу, значно прискорило процес постачання і зменшило зусилля на підтримку актуальності баз даних. Зазвичай для виконання EDI-транзакцій використовувалися приватні глобальні мережі, які були дешевшими, ніж виділені лінії, однак надавали сервіс надійної і безпечної доставки.

Internet забезпечує можливості взаємодії, необхідні для EDI, за низькими цінами. Але він не забезпечує сервісів безпеки (цілісності, конфіденційності, контролю учасників взаємодії), необхідних для EDI. Транзакції EDI вразливі до модифікації, компрометації або знищення при пересиланні через Internet.

Інформаційні транзакції – основний і дорогий елемент комерції. Інформація в комерції може мати декілька форм [12]:

- статичні дані, такі як історична інформація, карти і т.д.;
- корпоративна інформація, така як телефонні номери, адреси, структура організації тощо;
- інформація про продукцію або послуги;
- платна інформація, така як новини, періодичні видання, доступ до баз даних і т.д.

Використання Internet для надання таких сервісів значно дешевше, ніж використання факсу, телефону або звичайної пошти. Потенційні клієнти можуть шукати й одержувати інформацію в потрібному їм темпі, і це не вимагатиме додаткових витрат на службу технічного супроводу [11].

Зазвичай такі інформаційні сервіси використовують WWW як базовий механізм для надання інформації. Цілісність і доступність інформації, що надається, – головні проблеми забезпечення безпеки, що вимагають застосування засобів безпеки і створення політики безпеки [16].

Фінансові транзакції. Так чи інакше, але комп'ютери і мережі давно використовуються для обробки фінансових транзакцій. Переказ грошей з рахунку на рахунок в електронному вигляді використовується для транзакцій банк – банк, а банкомати – для операцій клієнт – банк. Авторизація покупця за допомогою кредитних карток виконується по телефонних лініях і мережах передавання даних [16–17]. Для підтримки безпеки ці транзакції виконуються через приватні мережі або шифруються. Використання приватних глобальних мереж (як і для EDI) обмежувало можливості взаємодії [13]. І тільки Internet надав дешеву можливість здійснювати фінансові транзакції. Існують три основні класи фінансових транзакцій та п'ять важливих типів механізму платежу (таблиця).

Платежі та фінансові трансакції

Взаємодія	Готівка	Чек	Дебет	Кредит	Електронний переказ фондів
Компанія-компанія		Основний			Допоміжний
Компанія-клієнт	Основний	Допоміжний	Допоміжний	Допоміжний	
Клієнт-клієнт	Основний	Допоміжний			

Застосування Internet для виконання цих типів транзакцій дає змогу замінити використання готівки, чеків, кредитних карток їх електронними еквівалентами. Основними визначеннями, що стосуються всіх класів безпеки електронної комерції, є експозиція, вразливість, атака, загроза, управління.

Експозицією називається форма можливої втрати або збитку для СЕК. Наприклад, експозиціями вважається неавторизований доступ до даних або протидія авторизованому використанню СЕК.

Уразливість – це деяка слабкість системи безпеки, яка може стати причиною нанесення пошкоджень СЕК.

Атакою називається дія деякого суб'єкта СЕК (користувача, програми, процесу і т.д.), що використовує вразливість комп'ютерної системи електронної комерції для досягнення цілей, які виходять за межі авторизації даного суб'єкта в комп'ютерній системі. Тобто, якщо, наприклад, користувач не має права на читання деяких даних, що зберігаються в системі електронної комерції, а йому цікаво їх знати і тому він виконує ряд відомих йому нестандартних маніпуляцій, що забезпечують доступ до цих даних (у разі відсутності або недостатньо надійної роботи засобів безпеки) або завершилися невдачею (у разі надійної роботи засобів безпеки), то цей користувач здійснює щодо СЕК атаку.

Загрозою для СЕК є умови, що створюють потенційну можливість нанесення СЕК збитку.

Управлінням у термінології безпеки називається захисний механізм (дія, пристрій, процедура, технологія тощо), що зменшує вразливість СЕК. Потрібно розуміти, що збиток СЕК – поняття також досить широке. Збитком уважається не тільки явне пошкодження будь-якого з компонентів СЕК, але і приведення СЕК в непрацездатний стан (наприклад, знеструмлення приміщення, в якому знаходяться апаратні засоби), різні витоки інформації (наприклад, незаконне копіювання програм, одержання конфіденційних даних), зміна деяких фізичних та логічних характеристик системи (наприклад, неавторизоване додавання записів до системних файлів і т.д.) Визначення можливого збитку СЕК – справа надто складна і залежить від багатьох умов: наприклад, від того, чи визнається юридично в даній країні так звана інтелектуальна власність або загальновідомий Copyright, чи розглядаються судами позови з відшкодування морального збитку, понесеного деякою особою або організацією внаслідок розголошування третьою стороною конфіденційної інформації і т.д.

Проблеми безпеки систем, що стосуються електронної комерції, можна умовно поділити на такі групи:

1. Проблеми забезпечення фізичної СЕК. До них належить захист систем від пожежі, затоплення, інших стихійних лих, збоїв живлення, крадіжки, пошкодження і т.д.
2. Проблеми забезпечення логічної безпеки СЕК. До них належить захист систем від неавторизованого доступу, від навмисних і ненавмисних помилок у діях людей і програм, які можуть призвести до збитку тощо.
3. Проблеми забезпечення соціальної безпеки компонентів СЕК. До них належать: розроблення законодавства, яке регулює застосування СЕК і визначає порядок розслідування та покарання за порушення їх безпеки; принципи і правила такої організації обслуговування користувачів у СЕК, яка зменшувала б ризик порушення безпеки систем і т.д.
4. Проблеми забезпечення етичної безпеки СЕК. Можливо, комусь це видасться не таким важливим, але багато фахівців уважають, що в забезпеченні безпеки СЕК чималу роль відіграють питання формування в користувачів певної дисципліни, а також формування конкретних етичних норм, обов'язкових для виконання всіма, хто працює з комп'ютерами. Наприклад, нещодавно експерти Національного наукового фонду США зробили спробу створити своєрідний "кодекс поведінки" фахівця у сфері ІС, зокрема систем електронної комерції. Вказувалося, що неетичними потрібно вважати будь-які навмисні або ненавмисні дії, які:

1) порушують нормальну роботу комп'ютерних систем;
2) викликають додаткові витрати ресурсів (машинного часу, лінії передачі тощо);
3) руйнують цілісність інформації, що зберігається й обробляється в комп'ютерних системах;
4) порушують інтереси легальних користувачів;
5) викликають незаплановані витрати ресурсів на ведення додаткового контролю, відновлення працездатності систем, видалення наслідків порушення безпеки систем та ін.

Як випливає з визначення ІС, зокрема систем електронної комерції, основними її компонентами є апаратні засоби, математичне (зокрема програмне) забезпечення і дані (інформація).

Теоретично існує лише чотири типи загроз для цих компонент:

§ ***переривання*** – при перериванні компонент системи втрачається (наприклад, унаслідок викрадення), стає недоступним (наприклад, унаслідок блокування – фізичного або логічного) або втрачає працездатність;

§ ***перехоплення*** – деяка третя неавторизована сторона отримує доступ до компонента. Прикладами перехоплення є незаконне копіювання програм і даних, неавторизоване читання даних з ліній зв'язку комп'ютерної мережі тощо.

§ ***модифікація*** – деяка третя неавторизована сторона не тільки отримує доступ до компонента, але і маніпулює ним. Наприклад, модифікаціями є неавторизована зміна даних у базах даних або взагалі у файлах комп'ютерної системи; зміна алгоритмів програм, що використовуються з метою виконання деякої додаткової незаконної обробки. Іноді модифікації виявляються досить швидко (якщо не відразу), але більш тонкі з них можуть залишатися невиявленими тривалий час;

§ ***підроблення*** – порушник може додати деякий фальшивий процес до системи для виконання потрібних йому, але не врахованих системою дій або підроблені записи у файли системи чи інших користувачів. Наприклад, знаючи формат запису в файлі, на основі якого у вашій організації нараховується зарплата, можна занести в цей файл підробний запис.

Такими є основні теоретичні принципи, необхідні для подальшого викладу всієї проблеми забезпечення безпеки СЕК.

Для забезпечення вказаних принципів необхідно на етапі проектування або вибору систем електронної комерції сформулювати вимоги до забезпечення режиму інформаційної безпеки при реалізації функцій і задач систем електронної комерції, а також розробити концепцію політики ІБ. При цьому після складання списку функцій і задач систем електронної комерції треба визначити вимоги до забезпечення режиму ІБ при їх реалізації. Ці вимоги формуються в термінах;

§ доступність;

§ цілісність;

§ конфіденційність.

Розробка концепції політики ІБ починається після вибору варіанта концепції систем електронної комерції, що створюється/вибирається і проводиться на основі аналізу таких груп чинників:

§ правові і договірні вимоги;

§ вимоги до забезпечення режиму ІБ за функціями і задачами системи електронної комерції;

§ загрози (класи ризиків), яких зазнають інформаційні ресурси.

Унаслідок аналізу формулюються загальні положення ІБ, що стосуються систем електронної комерції загалом:

§ цілі і пріоритети, які переслідує організація у сфері ІБ;

§ загальні напрями в досягненні цих цілей;

§ аспекти програми ІБ, які повинні вирішуватися на рівні всієї організації;

§ посадові особи та їх обов'язки щодо реалізації програми ІБ.

Потім розробляється політика ІБ, яка передбачає такі етапи:

§ аналіз ризиків;

§ визначення вимог до засобів захисту;

§ вибір основних рішень щодо забезпечення режиму ІБ;

§ розроблення планів забезпечення безперебійної роботи організації;

§ документальне оформлення політики ІБ.

Аналіз ризиків передбачає вивчення та систематизацію загроз ІБ, визначення вимог до засобів забезпечення ІБ [15] і здійснюється такими етапами:

§ вибір елементів системи електронної комерції та інформаційних ресурсів, для яких проводитиметься аналіз;

§ розроблення методології оцінки ризику;

§ аналіз загроз, визначення слабких місць у захисті;

§ аналіз і оцінка ризиків.

Вибір елементів системи електронної комерції та інформаційних ресурсів, для яких проводитиметься аналіз. На цьому етапі вибираються критичні елементи системи і критичні інформаційні ресурси, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення режиму ІБ [5–6].

Розроблення методології оцінки ризику. На цьому етапі повинні бути отримані оцінки граничнодопустимого та існуючого ризику здійснення загрози протягом певного часу. В ідеалі для кожної із загроз одержується значення ймовірності її здійснення протягом певного часу. Це допомагає співвіднести оцінку можливого збитку з витратами на захист. На практиці для більшості загроз неможливо отримати достовірні дані про ймовірність реалізації загрози і доводиться обмежуватись якісними оцінками. У розроблення методології оцінки ризику можуть бути використані методи системного аналізу.

Аналіз загроз, визначення слабких місць у захисті. Формується детальний список загроз, складається матриця загроз/елементів систем електронної комерції або інформаційних ресурсів. Кожному елементу матриці відповідає опис можливого впливу загрози на відповідний елемент системи або інформаційний ресурс. У процесі складання матриці уточнюється список загроз і виділених елементів.

Аналіз і оцінка ризиків. Цей етап передбачає такі кроки:

- оцінку збитку, пов'язану з реалізацією загроз. Оцінюється збиток, який може нанести діяльності організації реалізація загроз безпеки з урахуванням можливих наслідків порушення конфіденційності, цілісності і доступності інформації;
- оцінку витрат на заходи, пов'язані із захистом і залишкового ризику. Попередньо оцінюються прямі витрати за кожним заходом без урахування витрат на заходи, що мають комплексний характер;
- аналіз вартість/ефективність. Витрати на систему захисту інформації необхідно співвіднести з цінністю інформації, що захищається, й інших інформаційних ресурсів, що зазнають ризику, а також із збитком, який може бути нанесений організації через реалізацію загроз.

Унаслідок аналізу уточнюються допустимі залишкові ризики і витрати щодо заходів, пов'язаних із захистом інформації, і потім робляться висновки про допустимі рівні залишкового ризику і доцільність застосування конкретних варіантів захисту. За результатами проведеної роботи складається документ, що містить:

- переліки загроз ІБ,
- оцінки ризиків і рекомендації щодо зниження ймовірності їх виникнення і захисні заходи, необхідні для нейтралізування загроз.

Формування цілей та аналіз отриманих наукових результатів

Повторення незалежних випробувань у тексті. При дослідженні механізмів загроз ІБ результати окремої оцінки ризиків і рекомендацій не мають великого значення. Вивчення взаємодії системи, норми та ситуації експлікується за допомогою моделей теорії ймовірностей, які передбачають здійснення масового експерименту, у якому одна і та сама загроза ІБ (подія) повторюється багато разів. Ці випробування, що повторюються, утворюють серії, в кожній з яких подія з'являється або не з'являється певну кількість разів [4–5]. Вибір тієї чи іншої моделі опису оцінки ризиків залежить від побудови імовірнісного випробування і, зокрема, від організації вибору з переліку окремих його одиниць.

Повторна/безповторна вибірка. Розглянемо такий елементарний приклад. Нехай з переліку загроз ІБ взято N подій, серед яких n небезпечних з серйозними наслідками та m незначних загроз, і кожна з подій відбувалась на певному проміжку часу x_i разів ($i = \overline{1,k}$, $k = n + m$, $N = \sum_{i=1}^{k} x_i$); події відбулися без певної взаємозалежності, періодичності та черговості. Дослідження випробувань, які полягають у аналізі виконаних цих подій на певному проміжку часу, можуть здійснюватись за двома схемами.

За умовами першої схеми кожна виконана подія рахується такою, що може повторитись через деякий час, після того як у протоколі фіксується результат кожного випробування. При кожному наступному дослідженні випробування ймовірності появи тої чи іншої події залишаються незмінними. (Ці ймовірності відповідно дорівнюють *n/N* та *m/N*.). Ймовірнісно-зогрозливий експеримент, який оперує з наслідками взаємно незалежних випробувань, у кожному з яких події загроз зберігають свої безумовні ймовірності, називається *повторною вибіркою*.

При реалізації другої схеми виконані події вважаються такими, що повторюються. Ймовірність появи тієї чи іншої події у кожному наступному випробуванні залежить від результатів попередніх випробувань. ОТже, ми маємо справу з залежними випробуваннями, а ймовірність результату кожного з випробувань є умовною. Експеримент, який оперує з послідовністю залежних випробувань, у кожному з яких результати мають умовні ймовірності, називається *безповторною (або без повернень) вибіркою*.

Реальний ймовірнісно-загрозливий експеримент може бути здійснений як за допомогою повторної, так і за допомогою безповторної вибірки [9–10].

Три схеми незалежних випробувань загроз. Для дослідження загроз ІБ та оцінювання ризиків використовується метод серійного спостереження. Суть його полягає в тому, що одиниці загроз вибираються з фіксованого переліку групою: наприклад, по 3–5 загроз (подій) тощо. Одиниці загроз, які утворюють серію, не обов'язково повинні бути здійснені одна за однією, вони можуть бути виконані і через певний часовий інтервал.

При розв'язуванні багатьох теоретичних та інженерних задач часто потрібно знати ймовірність появи тієї чи іншої кількості певних одиниць загроз у серії. Якщо випробування ризиків, які утворюють серію, розглядаються як незалежні, то ми можемо здійснювати необхідне прогнозування за допомогою розроблених у теорії ймовірностей трьох систем незалежних випробувань: *простої*, *поліноміальної* та *пуассонівської*.

Проста схема передбачає тільки два результати досліду: появу або не появу ознаки *A*. Прикладом такої схеми є повторна вибірка з переліку загроз ІБ небезпечних (*A*) і незначних ($\overline{A}$) подій.

У *поліноміальній схемі* випробування дає не два, а декілька результатів. За цією схемою здійснюється, наприклад, експеримент, який полягає у виборі з переліку загроз ІБ подій трьох видів: з небезпечними наслідками, з середніми наслідками та незначних.

За *пуассонівською схемою* незалежні випробування здійснюються відносно декількох сукупностей (переривання, перехоплення, модифікація, підробка), у кожній з яких ознака має різну ймовірність. Тому ймовірність результату ризику змінюється алежно від того, відносно якої сукупності проводиться дослід.

Математична модель ризиків, за якою здійснюється прогнозування результатів простої схеми випробувань, є основою для побудови інших імовірнісних моделей, зокрема і тих, котрі широко використовуються у дослідженні переліку загроз ІБ.

Проста схема незалежних випробувань. Формула Бернуллі. Припустимо, що в деякій системи електронної комерції можливі виконання *n* загроз, своєю чергою, є *m* небезпечних загроз і *n-m* незначних. За схемою повторної вибірки проводиться *N* незалежних випробувань, які полягають у послідовному випадковому виконанні загрози з переліку можливих. Потрібно визначити ймовірність події, яка полягає в тому, що серед здійснених *N* загроз рівно *x* виявиться небезпечних, причому послідовність слідування небезпечної і незначної загроз не має значення.

Вважатимемо появу небезпечної загрози подією *A*, а появу незначної – подією $\overline{A}$. Визначимо ймовірності появи небезпечної та незначної. За класичним означенням ймовірності маємо:

$$P(A) = m/n = p,\ P(\overline{A}) = (n-m)/n = q.$$

Тепер знайдемо ймовірність того, що при *N* незалежних випробуваннях подія *A* з'явиться рівно *x* разів, якщо ймовірність появи цієї події при кожному окремому випробуванні стала і дорівнює *p*.

Для цього складемо всі можливі схеми, які утворять послідовність з появи x разів події A та $N-x$ разів непояви цієї події, тобто $AA\mathbf{K}A\ \overline{A}\,\overline{A}\mathbf{K}\overline{A}$. За теоремою множення ймовірність появи кожної схеми становить $p^x q^{N-x}$, а кількість таких схем дорівнює кількості сполук з N елементів по x, тобто C_N^x. Звідси випливає, що ймовірність появи події A рівно x разів у серії N незалежних випробувань становить

$$P_N(x)=C_N^x p^x q^{N-x}=\frac{N!}{x!(N-x)!}p^x q^{N-x}, \tag{1}$$

де $p+q=1$. Зауважимо також, що ймовірності (1) дорівнюють відповідним членам розкладу за формулою бінома виразу $(q+p)^N$.

За допомогою виразу (1), який називається *формулою Бернуллі*, і здійснюється імовірнісне прогнозування результатів за простою схемою незалежних випробувань.

Усі можливі несумісні між собою результати N дослідів полягають у появі 0, 1, 2,..., N разів події A. Тому сума величин (2.1), які є окремими значеннями ймовірностей при x=0, 1, 2, ..., N, дорівнює 1:

$$\sum_{x=0}^{N}P_N(x)=\sum_{x=0}^{N}C_N^x p^x q^{N-x}=(q+p)^N=1.$$

Розподіл ймовірностей $P_N(x)=C_N^x p^x q^{N-x}$ при x=0, 1, 2, ..., N називається *біноміальним розподілом* (або *біноміальним законом розподілу*) ймовірностей.

Часто, щоб одержати достатньо достовірні результати, доводиться проводити велику кількість незалежних випробувань. При цьому величини N та x можуть бути достатньо великими, що робить обчислення за щойно описаною схемою дуже важкими. У таких випадках обчислення ймовірностей $P_N(x)$ здійснюється за наближеними формулами.

Інколи для розв'язування інформаційної задачі необов'язково визначати всі ймовірності появи цієї події $0,1,2,\mathbf{K},N$ разів. Достатньо вказати найімовірнішгу кількість появ цієї події. Розглянемо відповідну схему. Зі збільшенням x величина $P_N(x)$ зростає, і при деякому x_0 (воно називається *модальним значенням*) досягає свого найбільшого значення $P_N(x_0)$. Після цього зі збільшенням x ймовірність $P_N(x)$ спадає.

Щоб визначити модальне значення x_0, розглянемо поведінку функції $P_N(x)$ послідовним порівнянням двох сусідніх членів розподілу. Нехай $P_N(x_0)$ – найбільше значення ймовірності у розподілі (1). Тоді виконуються такі дві нерівності:

$$P_N(x_0-1)\le P_N(x_0),\ P_N(x_0)\ge P_N(x_0+1). \tag{2}$$

Перепишемо першу з нерівностей (2) у вигляді

$$\frac{P_N(x_0)}{P_N(x_0-1)}=\frac{C_N^{x_0}p^{x_0}q^{N-x_0}}{C_N^{x_0-1}p^{x_0-1}q^{N-x_0+1}}=\frac{(N-x_0+1)p}{x_0 q}\ge 1. \tag{3}$$

Замінивши в останній нерівності q на $p-1$, одержимо

$$x_0\le Np+p. \tag{4}$$

Аналогічно, записавши другу з нерівностей (2) у вигляді

$$\frac{P_N(x_0+1)}{P_N(x_0)}=\frac{C_N^{x_0+1}p^{x_0+1}q^{N-x_0-1}}{C_N^{x_0}p^{x_0}q^{N-x_0}}=\frac{(N-x_0)p}{(x_0+1)q}\le 1, \tag{5}$$

одержимо

$$x_0\ge Np+p-1. \tag{6}$$

Об'єднуючи (4) та (6), отримуємо подвійну нерівність

$$Np+p-1\le x_0\le Np+p. \tag{7}$$

Знаючи модальне значення x_0, визначаємо потрібні нам імовірності біноміального розподілу. Обчислення їх починається з визначення максимальної ймовірності $P_N(x_0)$:

$$P_N(x_0) = C_N^{x_0} p^{x_0} q^{N-x_0} = \frac{N!}{x_0!(N-x_0)!} p^{x_0} q^{N-x_0}. \quad (8)$$

Обчислення решти ймовірностей здійснюється за такими рекурентними формулами, що побудовані на використанні виразів (3) та (5):

при $x < x_0$

$$\left.\begin{aligned} P_N(x_0-1) &= \frac{x_0}{N-(x_0-1)} \cdot \frac{q}{p} \cdot P_N(x_0), \\ P_N(x_0-2) &= \frac{x_0-1}{N-(x_0-2)} \cdot \frac{q}{p} \cdot P_N(x_0-1), \\ &\mathbf{L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L} \\ P_N(x_{\min}+1) &= \frac{x_0+2}{N-x_{\min}-1} \cdot \frac{q}{p} \cdot P_N(x_{\min}+2), \\ P_N(x_{\min}) &= \frac{x_{\min}+1}{N-x_{\min}} \cdot \frac{q}{p} \cdot P_N(x_{\min}+1), \end{aligned}\right\} \quad (9, \text{а})$$

при $x > x_0$

$$\left.\begin{aligned} P_N(x_0+1) &= \frac{N-x_0}{x_0+1} \cdot \frac{p}{q} \cdot P_N(x_0), \\ P_N(x_0+2) &= \frac{N-(x_0+1)}{x_0+2} \cdot \frac{p}{q} \cdot P_N(x_0+1), \\ &\mathbf{L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L\ L} \\ P_N(x_{\max}-1) &= \frac{N-(x_{\max}-2)}{x_{\max}-1} \cdot \frac{p}{q} \cdot P_N(x_{\max}-2), \\ P_N(x_{\max}) &= \frac{N-(x_{\max}-1)}{x_0+1} \cdot \frac{p}{q} \cdot P_N(x_{\max}-1), \end{aligned}\right\} \quad (9, \text{б})$$

де $x_{\min} \geq 0$ та $x_{\max} \leq N$.

Поліноміальна схема. Якщо випробування ризиків має декілька результатів, то їх імовірнісне прогнозування здійснюється за допомогою поліноміальної схеми. Її математична модель будується так.

Припустимо, що деяке випробування ризику може мати один з *k* різних попарно несумісних результатів A_1, A_2,..., A_k. Ймовірність кожного з них позначимо відповідно через $P(A_1) = p_1$, $P(A_2) = p_2$,..., $P(A_k) = p_k$. Оскільки подія $A_1 + A_2 + \mathbf{L} + A_k$ є достовірною, то $p_1 + p_2 + \mathbf{L} + p_k = 1$. Здійснимо *N* незалежних випробувань і визначимо ймовірності того, що подія A_1 з'явиться x_1 разів, подія A_2 – x_2 разів,..., подія A_k – x_k разів, де $x_1 + x_2 + \mathbf{L} + x_k = N$.

Вказаний результат одержується різними шляхами, кожний з яких відповідає різним переставленням x_1 разів результату A_1, x_2 разів результату A_2,..., x_k разів результату A_k. Ймовірність появи кожної такої комбінації дорівнює $p_1^{x_1} p_2^{x_2} \mathbf{L}\, p_k^{x_k}$. Загальна кількість таких комбінацій дорівнює добутку $C_N^{x_1} C_N^{x_2} \mathbf{L}\, C_N^{x_k}$, який приводиться до виразу

$$\frac{N!}{x_1! x_2! \mathbf{L}\, x_k!}.$$

Звідси одержуємо, що при N незалежних випробуваннях ймовірність одержати x_1 разів результат A_1, x_2 разів результат A_2,..., x_k разів результат A_k дорівнює

$$P_N(x_1, x_2, \mathbf{K}, x_k) = \frac{N!}{x_1! x_2! \mathbf{L}\, x_k!} \cdot p_1^{x_1} p_2^{x_2} \mathbf{L}\, p_k^{x_k}, \qquad (10)$$

де $0 \le x_i \le N$, а $\sum_{i=1}^{k} x_i = N$.

У частковому випадку, коли $k = 2$, маємо

$$P_N(x_1, x_2) = \frac{N!}{x_1! x_2!} \cdot p_1^{x_1} p_2^{x_2}.$$

Враховуючи, що $x_1 + x_2 = N$, а $p_1 + p_2 = 1$, і позначаючи x_1 через x, x_2 – через $N - x$, p_1 – через p, а p_2 – через q, приходимо до виразу

$$P_N(x) = \frac{N!}{x!(N-x)!} p^x q^{N-x} = C_N^x p^x q^{N-x},$$

тобто до формули Бернуллі для простої системи схеми незалежних випробувань. Отже, формула Бернуллі є частинним випадком співвідношення (10).

Як і проста схема, поліномна схема використовується у повторних вибірках ризиків за умови, що величини $N, x_1, x_2, \mathbf{K}, x_k$ не дуже великі. За цих умов використання розглянутої схеми дає цінну інформацію не тільки для ймовірнісної побудови алгоритмів системного аналізу переліку загроз ІБ в системах електронної комерції. Ці алгоритми дають також змогу визначити оптимальну послідовність оцінки ризиків та проведення рекомендацій щодо зниження ймовірності їх виникнення і захисні заходи, необхідні для нейтралізування загроз в системах електронної комерції.

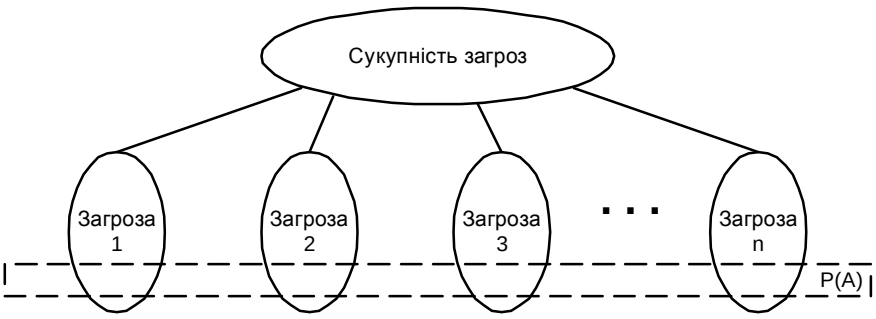
Пуассонівська схема. У практиці ІБ часто доводиться мати справу з такою сукупністю загроз, у якій транзакції, що її складають, належать до різних типів загроз. Оскільки перелік загроз будуються, виходячи з різних норм, то кожна одиниця загроз має в кожному переліку свою апріорну ймовірність. У підсумку ймовірності появи та не появи певних одиниць міняються від досліду до досліду в системах електронної комерції.

Така ситуація, зображена на рисунку, описується *схемою Пуассона*. Формальне подання цієї схеми ґрунтується на таких міркуваннях.

Нехай здійснюється N незалежних випробувань, у кожному з яких може з'явитись або не з'явитись подія A. Ймовірності появи події A в 1, 2, ..., N випробуваннях відповідно дорівнюють $p_1, p_2, \mathbf{K}, p_N$, а ймовірності її непояви дорівнюють $q_1 = 1 - p_1$, $q_2 = 1 - p_2$, $q_N = 1 - p_N$. Можна показати, що ймовірність появи результату A в серії з N випробувань рівно x разів становить

$$P_N(x) = p_1 p_2 p_3 \mathbf{K}\, p_x q_{x=1} \mathbf{K}\, q_N + p_1 q_2 p_3 \mathbf{K}\, q_{N-1} p_N + \mathbf{L} + q_1 q_2 q_3 \mathbf{K}\, q_{N-x} p_{N-x+1} p_{N-x+2} \mathbf{K}\, p_N. \qquad (11)$$

Отже, потрібна ймовірність є сумою всіх можливих добутків, у кожному з яких p з різними індексами міститься рівно x разів, а q з різними індексами входить $N - x$ разів.



Пуассонівська схема появи сукупності загроз інформаційної безпеки в системах електронної комерції

Щоб утворити всі можливі добутки з x ймовірностей p_i та $N-x$ ймовірностей q_i $(i=1, 2, \mathbf{K}, N)$, утворимо добуток біномів

$$(q_1 + p_1 t)\ (q_2 + p_2\ \ t)\ \mathbf{L}\ (q_N + p_N\ \ t) = \prod_{i=1}^{N} (q_i + p_i\ \ t), \qquad (12)$$

де t – деякий довільний параметр.

Перемножимо біноми і зведемо подібні члени, тоді одержимо рівність

$$\prod_{i=1}^{N} (q_i + p_i t) = \sum_{x=0}^{N} P_N(x) t^x,$$

у якій коефіцієнт при t^x є ні що інше, як вираз (11).

Розкриємо дужки у лівій частині рівності й зведемо подібні члени, тоді отримаємо всі ймовірності $P_N(0)$, $P_N(1)$, $P_N(2)$, ..., $P_N(N)$, котрі виступають у ролі коефіцієнтів, відповідно, при t^0, t^1, t^2, ..., t^N. Сума всіх ймовірностей $P_N(x)$ дорівнює 1:

$$\sum_{x=0}^{N} P_N(x) = 1.$$

Зокрема, якщо $p_1 = p_2 = \mathbf{K} = p_N = p$, $q_1 = q_2 = \mathbf{K} = q_N = q$, маємо

$$(q + pt)^N = \sum_{x=0}^{N} C_N^x p^x q^{N-x} t^x,$$

звідки випливає формула Бернуллі. Схему Пуассона, як і дві попередні схеми, доцільно використовувати в випробуванні ризиків тоді, коли ми можемо організувати повторну вибірку, а величини N та x не дуже великі.

Визначення вимог до заходів захисту і вибір основних рішень щодо забезпечення режиму ІБ. Визначення вимог до засобів захисту передбачає такі етапи:

§ Формулювання вимог до ІБ, аналізуючи функції і задачі ІС з урахуванням проведеного аналізу ризиків. Вимоги до ІБ формулюються в термінах функцій і механізмів безпеки;

§ Вибір профілю захисту (класу захищеності системи електронної комерції від несанкціонованого доступу (НСД)).

У виборі основних рішень щодо забезпечення режиму ІБ структурується комплекс заходів за рівнями:

§ адміністративному (забезпечення розробки і виконання програми ІБ);

§ організаційному (організація роботи персоналу і регламентація його дій);

§ програмно-технічному (програмно-технічна реалізація механізмів безпеки).

На **адміністративному рівні забезпечення ІБ** повинні бути вироблені:

§ система підтримки керівництвом організації заходів щодо забезпечення ІБ, виконання правових і договірних вимог у сфері ІБ;

§ процедура доведення до відома співробітників основних положень концепції ІБ, вимоги щодо навчання персоналу правилам ІБ;

§ система контролю за реалізацією прийнятих рішень і відповідальні посадові особи.

На **організаційному рівні забезпечення ІБ** мають бути розглянуті:

§ організаційна структура служби, що відповідає за забезпечення режиму ІБ, розподіл обов'язків;

§ комплекс профілактичних заходів (попередження появи вірусів, попередження ненавмисних дій, які призводять до порушення ІБ);

§ організація доступу співробітників сторонніх організацій до ресурсів системи електронної комерції;

§ організація доступу користувачів і персоналу до конкретних ресурсів системи електронної комерції;

§ політика щодо окремих аспектів: віддалений доступ до системи електронної комерції, використання відкритих ресурсів (наприклад, Інтернет), використання несертифікованого програмного забезпечення (ПЗ) тощо.

На **програмно-технічному рівні забезпечення ІБ** розглядаються програмно-технічні засоби, які реалізують задані вимоги. Якщо вимоги формулювалися в термінах функцій (сервісів) безпеки, розглядаються механізми безпеки і відповідні їм варіанти програмних і апаратних реалізацій [16, 17]. Якщо вимоги формулювалися за підсистемами ІС, розглядаються варіанти програмно-апаратної реалізації цих підсистем. Під час розгляду різних варіантів рекомендується враховувати такі аспекти:

§ управління доступом до інформації і сервісів, враховуючи вимоги до розподілу обов'язків і ресурсів;

§ реєстрація подій у журналі з метою щоденного контролю або спеціальних розслідувань;

§ перевірка і забезпечення цілісності критично важливих даних на всіх стадіях їх опрацювання;

§ захист конфіденційних даних від несанкціонованого доступу, зокрема використання засобів шифрування;

§ резервне копіювання критично важливих даних;

§ відновлення роботи системи електронної комерції після відмов, особливо для систем з підвищеними вимогами щодо доступності;

§ захист від внесення несанкціонованих доповнень і змін;

§ забезпечення засобів контролю, наприклад, за допомогою використання програм у вибірковому контролі та альтернативні варіанти програмного забезпечення для повторення критично важливих обчислень.

Висновки і перспективи подальших наукових розвідок

Для забезпечення захисту інформації електронної комерції необхідно і достатньо, щоб зміна станів системи спричиняла тільки їх безпечність, якщо початковий стан був безпечним. Сьогодні захист інформації, представленої в електронному вигляді, від таких методів впливу: запитів на читання, на запис, на модифікацію, на створення об'єкта без збереження узгодженості, на знищення, на зміну свого поточного рівня захисту. Для ефективного захисту інформації в системах електронної комерції використовують програмно-апаратні засоби захисту програмного забезпечення від несанкціонованого доступу і копіювання. Авторами запропоновано прогнозування результатів масових випробувань ризиків в системах електронної комерції. Такі прогнози поки що можна здійснювати стосовно повторних вибірок, спираючись на класичне означення ймовірності, тобто за умови, що дослід здійснюється відносно порівняно обмеженої за обсягом сукупності об'єктів. Така ситуація зустрічається у ІБ порівняно рідко. Найчастіше ІБ доводиться мати справу з безповторною вибіркою, яка досліджує одиниці загроз, що рідко зустрічаються. За таких умов розподіл ймовірностей появи загрози (події) підпорядковується гіпергеометричному закону.

1. Береза А.М. Електронна комерція. – К, 2002. 2. Галіцин В.К., Левченко Ф.А. Багатокористувальницькі обчислювальні системи та мережі. – К.: КНЕУ, 1997. 3. Грабовый П.Г., Петрова С.Н., Полтавцев С.И., Романова К.Г., Хрусталев В.Б., Яровенко С.М. – М.: Аьянс, 1994. 4. Джерк Н. Разработка приложений для электронной коммерции. – СПб.: Питер, 2001. 5. Катренко А.В. Ситемний аналіз об'єктів та процесів комп'ютерізації. – Львів: "Новий світ – 2000", 2003. –С. 286 – 322. 6. Катренко А.В. Системні аспекти розвитку архітектури підприємства // Вісн. Нац. ун-ту "Львівська політехніка". – 2002. – №464. – С. 123–131. 7. Козьє Девид, Электронная коммерция. – М.: Русская Редакция, 1999. 8. Крупник А. Бизнес в интернет. – М.: Микроарт, 2002. 9. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. 10. Советов Б.Я. Яковлев С.А. Моделирование систем. – М.: Высшая школа, 1985. 11. Успенский И.Энциклопедия Интернет-бизнеса. – СПб.: Питер, 2001. 12. Холмогоров В. Интернет – маркетинг. – СПб.: Питер, 2001. 13. Эймор Дэниел, Электронный бизнес. Эволюция и/или революция. – М.: Вильямс, 1999. 14. Рішняк І.В. Системний аналіз категорій ризику та невизначеності // Вісн. Нац. ун-ту "Львівська політехніка". – 2003. – № 489. 15. Верес О.М., Катренко А.В., Рішняк І.В., Чаплига В.М. Управління ризиками в проектній діяльності // Вісн. Нац. ун-ту "Львівська політехніка". – 2003. – №489. – С.38–49. 16. Берко А.Ю., Висоцька В.А., Чирун Л.В. Алгоритми опрацювання інформаційних ресурсів в системах електронної комерції // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 519. – С.10–20. 17. Берко А.Ю., Висоцька В.А. Проектування навігаційного графу web-сторінок бази даних систем електронної комерції // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 521. – С.48–57.