УДК 004.413.4, 004.942, 007.5, 65.011.3, 681.518

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

АНАЛІЗ ЯКІСНИХ ТА КІЛЬКІСНИХ ХАРАКТЕРИСТИК ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Проаналізовано поняття інформації в аспекті об'єкта права власності та досліджено загрози інформаційній безпеці при проектуванні систем захисту інформації.

The analysis of concept of information in the aspect of object of right of ownership is conducted and threats informative safety at planning of the systems of priv are investigational in the article.

Загальна постановка проблеми

Останнім часом повідомлення про атаки на інформацію, «хакерів» та зламування комп'ютерів все частіше з'являються у засобах масової інформації. Що ж таке «атака на інформацію»? Дати визначення цій дії насправді дуже складно, оскільки інформація, особливо електронна, представлена сотнями різних видів. Інформацією можна вважати й окремий файл, і базу даних, і один запис у ній, і цілий програмний комплекс. І всі ці об'єкти можуть бути «атаковані» певними особами чи групами осіб. При збереженні, підтримці і наданні доступу до будь-якого інформаційного об'єкта його власник чи уповноважена ним особа накладає певні вимоги чи правила роботи з нею. Навмисне порушення цих правил розцінюється як атака на інформацію.

Розглядаючи інформацію як об'єкт захисту, треба зазначити, що інформація – це результат відображення і опрацювання у людській свідомості різноманіття навколишнього світу, це відомості про навколишні предмети, явища природи, діяльність інших людей тощо. Інформація, якою люди обмінюються через інформаційні системи (ІС), є предметом захисту. Захисту потребує не лише таємна інформація. Модифікація несекретних даних може призвести до витоку таємних. Знищення або зникнення накопичених з великими труднощами даних може призвести до їх безнадійної втрати.

Залежно від сфери і масштабів застосування тієї чи іншої системи опрацювання даних втрата або витік конфіденційної інформації може призвести до різноманітних за важливістю наслідків: від невинних жартів до надзвичайних наслідків економічного та політичного характеру. Особливо поширені злочини в автоматизованих системах, які обслуговують банківські та торговельні структури.

Практична задача забезпечення інформаційної безпеки (ІБ) полягає в розробленні моделі представлення системи (процесів) ІБ, яка на основі науково-методичного апарату давала б змогу вирішувати завдання створення, використання й оцінювання ефективності систем захисту інформації (СЗІ) для проектованих та існуючих ІС.

Зв'язок висвітленої проблеми із важливими науковими та практичними завданнями

З масовим впровадженням комп'ютерів в усі сфери діяльності людини обсяг інформації, збереженої в електронному вигляді, зріс у тисячі разів. Зараз скопіювати і віднести дискету з файлом, що містить план випуску продукції, набагато простіше, ніж переписувати сотні паперів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією цілісності інформації.

Які можливі наслідки атак на інформацію? Насамперед, звичайно, нас цікавитимуть економічні втрати:

1. Розкриття комерційної інформації може призвести до серйозних прямих збитків на ринку.

2. Звістка про крадіжку великого обсягу інформації серйозно впливає на репутацію фірми, приводячи до втрат в обсягах торгових операцій.

3. Фірми-конкуренти можуть скористатися крадіжкою інформації, якщо та залишилася непоміченою, для того щоб довести фірму до банкрутства, нав'язуючи їй фіктивні або свідомо збиткові угоди.

4. Підміна інформації як на етапі передачі, так і на етапі збереження у фірмі може призвести до величезних збитків.

5. Багаторазові успішні атаки на фірму, що надає будь-який вид інформаційних послуг, зменшують довіру до фірми в клієнтів, що позначиться на обсязі прибутків.

Природно, комп'ютерні атаки можуть принести і величезний моральний збиток. Поняття конфіденційного спілкування давно вже стало притчею. Зрозуміло, що будь-який користувач комп'ютерної мережі не хоче, щоб його листи, крім адресата, одержували ще 5–10 осіб або, наприклад, весь текст, що набирається на клавіатурі ПК, копіювався в буфер, а потім, під час під'єднання до Інтернету, відправлявся на визначений сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Основним завданням моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильного оцінювання ефективності прийнятих рішень і вибору раціонального варіанта технічної реалізації системи захисту інформації.

Специфічними особливостями вирішення завдання створення систем захисту є:

1. ***Неповнота і невизначеність вихідної інформації*** про склад ІС і характерні загрози;

2. ***Багатокритерійність задачі***, пов'язана з необхідністю обліку великої кількості показників (вимог) СЗІ;

3. ***Наявність кількісних та якісних показників***, які необхідно враховувати під час розв'язання задач розроблення і впровадження СЗІ;

4. ***Неможливість застосування класичних методів оптимізації***.

Розроблювана модель повинна задовольняти такі вимоги:

a. Використовуватися як:
   - Посібник зі створення СЗІ;
   - Методика формування показників і вимог до СЗІ;
   - Інструмент (методика) оцінки СЗІ;
   - Модель СЗІ для проведення досліджень (матриця стану);

b. Мати такі властивості:
   - Універсальність;
   - Комплексність;
   - Простота використання;
   - Наочність;
   - Практична спрямованість;
   - Самонавчальність (можливість нарощування знань);
   - Функціонування в умовах високої невизначеності вихідної інформації;

c. Давати змогу:
   - Установити взаємозв'язок між показниками (вимогами);
   - Задавати різні рівні захисту;
   - Одержувати кількісні оцінки;
   - Контролювати стан СЗІ;
   - Застосовувати різні методики оцінок;
   - Оперативно реагувати на зміни умов функціонування;
   - Об'єднати зусилля різних фахівців єдиним задумом.

Аналіз сучасних досліджень і публікацій

Цінність інформації є критерієм при прийнятті будь-якого рішення про її захист. Хоча було зроблено багато різних спроб формалізувати цей процес з використанням методів теорії інформації

і аналізу рішень, процес оцінки досі залишається вельми суб'єктивним. Для оцінки потрібний розподіл інформації на категорії відповідно не тільки до її цінності, але й важливості. Відомим є такий розподіл інформації за ступенем важливості [7]:

1) життєво важлива незамінна інформація, наявність якої необхідна для функціонування організації;

2) важлива інформація – інформація, яка може бути замінена або відновлена, але процес відновлення дуже важкий і пов'язаний з великими витратами;

3) корисна інформація – інформація, яку важко відновити, однак організація може ефективно функціонувати й без неї;

4) несуттєва інформація – інформація, яка організації більше не потрібна.

На практиці віднесення інформації до однієї з цих категорій є досить складним завданням, оскільки одна й та сама інформація може бути використана багатьма підрозділами організації, кожен з яких може зарахувати її до різних категорій важливості. Категорія важливості, як і цінність інформації, згодом змінюється й залежить від ставлення до неї різних груп споживачів і потенційних порушників. Існують визначення груп осіб, які пов'язані з опрацюванням інформації: утримувач – організація або особа, що є власником інформації; джерело – організація або особа, що постачає інформацію; порушник – особа або організація, які незаконно прагнуть отримати інформацію. Ставлення цих груп до значущості однієї й тієї ж інформації може бути різним. Наприклад:

- важлива оперативна інформація, наприклад, список замовлень на поточний тиждень і графік виробництва, може мати для користувача високу цінність, тоді як для джерела або порушника – низьку;
- персональна інформація, наприклад, медична, має значно більшу цінність для джерела (особи, якої стосується інформація), ніж для її користувача або порушника;
- інформація, що використовується керівництвом для розроблення і прийняття рішень, наприклад, про перспективи розвитку ринку, може бути значно ціннішою для порушника, ніж для джерела або її утримувача, який вже завершив аналіз цих даних.

Наведені категорії важливості заслуговують на увагу і можуть бути застосовані до будь-якої інформації. Це також узгоджується з існуючим принципом розподілу інформації за рівнями таємності. Рівень таємності – це адміністративна або законодавча міра, адекватна мірі відповідальності особи за витік або втрату конкретної таємної інформації, що регламентується спеціальним документом з урахуванням державних, військово-стратегічних, комерційних, службових або приватних інтересів. Такою інформацією може бути державна, військова, комерційна, службова або особиста таємниця.

Практика свідчить, що захищати необхідно не тільки таємну інформацію. Несекретна інформація, піддана несанкціонованим змінам (наприклад, модифікації команд управління), може призвести до витоку або втрати пов'язаної з нею таємної інформації, а також до невиконання автоматизованою системою заданих функцій внаслідок отримання помилкових даних, які можуть бути не виявлені користувачем системи.

Сумарна кількість або статистика нетаємних даних в результаті може виявитися таємною. Аналогічно, зведені дані одного рівня таємності загалом можуть бути інформацією вищого рівня таємності. Для захисту від подібних ситуацій широко застосовується розмежування доступу до інформації за функціональною ознакою. За однакового ступеня важливості інформація, що опрацьовується системою, поділяється відповідно до функціональних обов'язків і повноважень користувачів.

До останнього часу безпека інформації в автоматизованих системах (АС) трактувалася винятково як небезпека несанкціонованого отримання інформації протягом усього часу опрацювання і зберігання в АС. Сьогодні безпека інформації інтерпретується ще й як безпека дій, для виконання яких використовується інформація. Принципові відмінності розширеного тлумачення, на відміну від традиційного, дуже важливі, оскільки обчислювальна техніка все більше використовується для автоматизованого управління інформаційними системами і процесами, в яких несанкціоновані зміни запланованих алгоритмів і технологій можуть мати серйозні наслідки.

Історично традиційним об’єктом права власності є матеріальний об’єкт. Інформація не є матеріальним об’єктом, інформація – це знання, тобто відображення дійсності в свідомості людини (причому істинне або помилкове відображення – не істотно, важливо, що в свідомості). Надалі інформація може втілюватися в матеріальні об’єкти навколишнього світу.

Як нематеріальний об’єкт, інформація нерозривно пов’язана з матеріальним носієм. Це – мозок людини або відчужені від людини матеріальні носії, такі, як книга, дискета й інші види “пам’яті” (запам’ятовувальні пристрої комп’ютера).

З філософського погляду можна, мабуть, говорити про інформацію як про абстрактну субстанцію, існуючу саму по собі, але для нас ні зберігання, ні передача інформації без матеріального носія неможливі. Як наслідок:

a. Інформація як об’єкт права власності копіюється (тиражується) за рахунок матеріального носія. Матеріальний об’єкт права власності не копіюється. Дійсно, якщо розглянути дві однакові речі, то вони складаються з однакових структур, але матеріально різних молекул. А інформація під час копіювання залишається тією самою, це – те саме знання, та сама семантика.

b. Інформація як об’єкт права власності легко переміщується до іншого суб’єкта права власності без помітного порушення права власності на інформацію. Переміщення матеріального об’єкта до іншого суб’єкта права власності неминуче і, як правило, спричиняє втрату цього об’єкта первинним суб’єктом права власності, тобто відбувається очевидне порушення його права власності.

Небезпека копіювання і переміщення інформації посилюється тим, що вона зберігається і опрацьовується в сфері доступності значної кількості суб’єктів, які не є суб’єктами права власності на неї. Це, наприклад, автоматизовані системи, зокрема й інформаційні мережі.

Розглянувши особливості інформації, можна зробити висновок, що як об’єкт права власності інформація нічим не відрізняється від традиційних об’єктів права власності. Право власності містить три складові елементи права власності: право розпорядження; право володіння; право користування. Суб’єкт права власності на інформацію може передати частину своїх прав (розпорядження), не втрачаючи їх сам, іншим суб’єктам, наприклад – власникові матеріального носія інформації (це – володіння або користування) або користувачеві (це – користування і, можливо, володіння).

Для інформації право розпорядження передбачає виняткове право (ніхто інший, крім власника) визначати, кому ця інформація може бути надана у володіння чи користування.

Сутність проблеми та формування цілей

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, при 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 [5]. Вибір тієї чи іншої моделі опису оцінки ризиків залежить від побудови імовірнісного випробування і, зокрема, від того, як організовано вибір з переліку окремих його одиниць.

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 вважається такою, що може повторитися через деякий час, після того, як у протоколі фіксується результат кожного випробування. При кожному наступному дослідженні випробування ймовірності появи тієї чи іншої події залишаються незмінними і відповідно дорівнюють n/N та m/N. Ймовірнісно-загрозливий 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 не 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 [8]. Дослідження загроз ІБ та проведення оцінювання ризиків використовує метод серійного спостереження. Суть його полягає в тому, що події (загрози) вибираються з фіксованого переліку групою: наприклад, по 3–5 подій (загроз) тощо. Події, які утворюють серію, необов'язково повинні бути здійсненні одна за однією, вони можуть реалізуватись через певний часовий інтервал.

Аналіз отриманих результатів

Під час розв'язування багатьох теоретичних та інженерних задач часто потрібно знати ймовірність появи тієї чи іншої кількості певних подій у серії. Якщо випробування ризиків, які утворюють серію, розглядаються як незалежні, то ми можемо здійснювати необхідне прогнозування за допомогою розробленого гіпергеометричного закону.

Математична модель ризиків, за якою здійснюється прогнозування результатів гіпергеометричного закону випробувань, є основою для побудови інших імовірнісних моделей, зокрема і тих, котрі широко використовуються у дослідженні переліку загроз ІБ. Розглянуті вище властивості описували числові особливості серії з кількох вибірок.

Проаналізуємо якісні та кількісні характеристики, якими володіє одна вибірка.

Нехай B'_x – подія, яка полягає в тому, що загроза ІБ *A* з'явиться не менше *a* і не більше *b* разів. Тоді ймовірність $P_N(a \le x \le b)$ цієї події становитиме

$$P_N(a \le x \le b) = P_N(a) + P_N(a+1) + \cdots + P_N(b-1) + P_N(b) = \sum_{x=a}^{b} P_N(x) = \sum_{x=a}^{b} C_N^x p^x q^{N-x}.$$

Графічно кількість доданків, які необхідно обчислити, можна зобразити так (рис. 1):

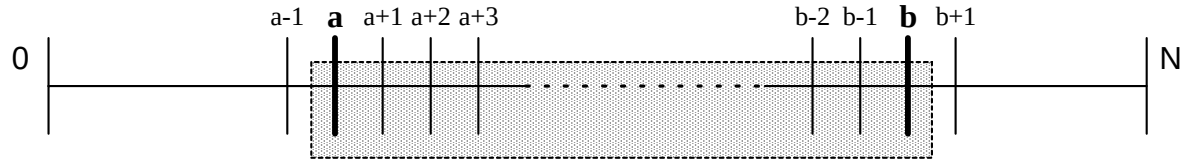

Рис. 1. Графічне відображення кількості доданків при імовірності $P_N(a \le x \le b)$ події

Якщо кількість членів, які відповідають значенням *x* від *a* до *b*, значно більша за загальну кількість членів, що відповідають значенням *x* від 0 до $a-1$ і від $b+1$ до *N*, то зручніше підсумовувати ймовірності за цими двома послідовностями. У такому разі одержуємо ймовірність протилежної події $\overline{B'_x}$:

$$P\left(\overline{B'_x}\right) = \sum_{x=0}^{a-1} C_N^x p^x q^{N-x} + \sum_{x=b+1}^{N} C_N^x p^x q^{N-x}.$$

Тепер потрібну нам імовірність обчислюємо за формулою

$$P_N(a \le x \le b) = 1 - P\left(\overline{B'_x}\right) = 1 - \sum_{x=0}^{a-1} C_N^x p^x q^{N-x} - \sum_{x=b+1}^{N} C_N^x p^x q^{N-x}. \quad (1)$$

Графічно такий підхід можна інтерпретувати так (рис 2):

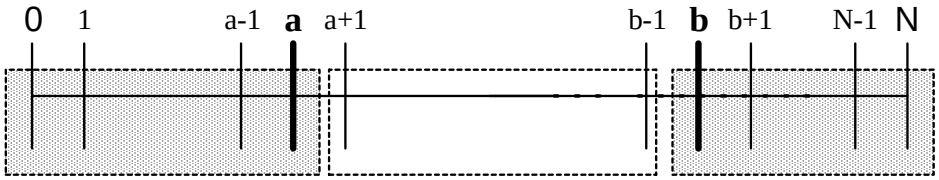

Рис. 2. Графічне відображення кількості доданків при імовірності $P_N(a \le x \le b)$ протилежної події

Розглянемо деякі часткові випадки.

Припустимо, що необхідно визначити ймовірність того, що деяка одиниця загрози *A* зустрінеться не менше *a* разів. Тут

$$P_N(x \ge a) = \sum_{x=a}^{N} C_N^x p^x q^{N-x} .$$

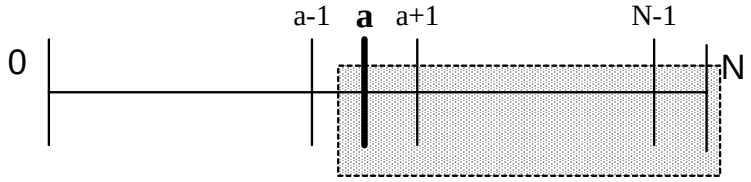

Рис. 3. Графічне відображення кількості доданків при імовірності $P_N(x \ge a)$ події

Якщо значення *a* мале, то доцільно скористатись виразом

$$P_N(x \ge a) = 1 - \sum_{x=0}^{a-1} C_N^x p^x q^{N-x} ,$$

який є частинним випадком формули (1).

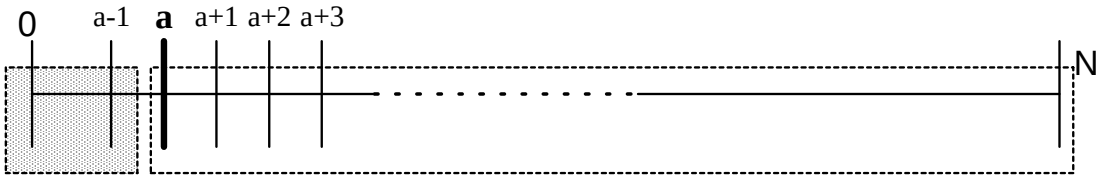

Рис. 4. Графічне відображення кількості доданків при імовірності $P_N(x \ge a)$ протилежної події

У тому випадку, коли $a = 1$, маємо

$$P_N(1 \le x \le N) = 1 - C_N^0 p^0 q^N = 1 - q^N . \qquad (2)$$

Імовірність появи події *A* не більше *b* разів також визначається шляхом підсумовування ймовірностей, у яких подія з'являється 0, 1, 2, ..., *b* разів:

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

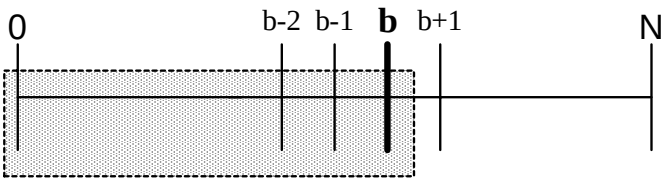

Рис. 5. Графічне відображення кількості доданків при імовірності $P_N(x \le b)$ події

Якщо значення *b* близьке до *N*, то цю ймовірність доцільно обчислювати за такою формулою:

$$P_N(x \le b) = 1 - \sum_{x=b+1}^{N} C_N^x p^x q^{N-x}, \qquad (3)$$

яка також є частинним випадком формули (1).

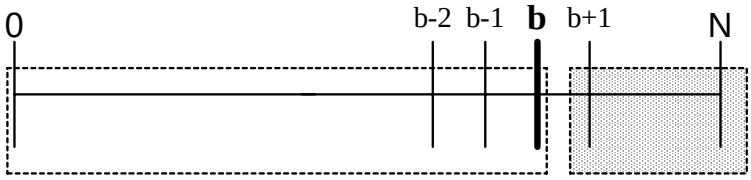

Рис. 6. Графічне відображення кількості доданків при імовірності $P_N(x \le b)$ протилежної події

У дослідженнях загроз ІБ і особливо при проектуванні систем захисту інформації в системах електронної комерції постійно виникає потреба визначати обсяг можливих загроз, необхідний для того, щоб забезпечити із заданою ймовірністю захист інформаційних та фінансових транзакцій.

Для цього перетворимо спочатку формулу

$$P_N(1 \le x \le N) = 1 - q^N = 1 - (1-p)^N$$

до вигляду

$$(1-p)^N = 1 - P_N(1 \le x \le N).$$

Прологарифмуємо обидві частини рівності і після нескладних перетворень одержимо

$$N = \frac{\lg[1 - P_N(1 \le x \le N)]}{\lg(1-p)}, \qquad (4)$$

де *N* вказує на необхідний обсяг вибірки.

Висновки

Інформація є об’єктом права власності і, відповідно, потребує захисту від несанкціонованого доступу, знищення та тиражування. Для прогнозування ймовірності загроз для ІБ можна використовувати метод серійного спостереження. Реальний експеримент може бути здійснений за допомогою як повторної, так і безповторної вибірки. Якщо випробування ризиків, які утворюють серію, розглядаються як незалежні, то можна здійснювати необхідне прогнозування за допомогою гіпергеометричного закону.

1. Берко А.Ю., Висоцька В.А., Чирун Л.В. Алгоритми опрацювання інформаційних ресурсів в системах електронної комерції // Вісник Нац. ун-ту “Львівська політехніка”. Інформаційні системи та мережі. – 2004. – № 519. – С.10–20. 2. Берко А.Ю., Висоцька В.А. Проектування навігаційного графу web – сторінок бази даних систем електронної комерції // Вісник Нац. ун-ту “Львівська політехніка”. Комп’ютерні науки та інформаційні технології. – 2004. – № 521. – С.48–57. 3. Береза А.М. Електронна комерція. – К., 2002. 4. Верес О.М., Верес О.О., Рішняк І.В. Методи оцінки та моделі управління банківськими ризиками // Вісник Нац. ун-ту “Львівська політехніка”. Інформаційні системи та мережі.-2004.-№519. 5. Катренко А.В. Ситемний аналіз об’єктів та процесів комп’ютерізації. – Львів: “Новий світ – 2000”, 2003. – С. 286–322. 6. Крупник А. Бизнес в интернет. – М.: Микроарт, 2002. 7. Рішняк І.В. Роль інформації в управлінні ризиками прийняття рішень // Вісник Нац. ун-ту “Львівська політехніка” „Інформаційні системи та мережі”. – 2004. – №519. 8. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. 9. Успенский И. Энциклопедия Интернет-бизнеса. – СПб.: Питер, 2001.