# OPTIMIZAREA SISTEMELOR DE SECURITATE INFORMAȚIONALĂ UTILIZÎND TEORIA PROBABILITĂȚILOR

**Autori: Nicoleta DUCA**
**Cond. şt. Rodica BULAI**

**Universitatea Tehnică a Moldovei**
Email: nicoleta.duca@mail.ru, rodica.bulai@ati.utm.md, griniuc@yahoo.com

***Abstract:*** *Securitatea informațională la moment reprezintă una dintre direcțiile prioritare ale bussinesului, dat fiind faptul că perturbările care survin în această sferă se soldează, în marea majoritate a cazurilor, cu efecte catastrofale pentru orice organizație. Posibilitățile care le oferă tehnologiile informaționale creează condiții favorabile pentru progresarea afacerilor, însă pe de ală parte, creează premise reale de scurgere a informației, sustragere, falsificare, distrugere sau copiere şi ca rezultat provocînd daune economice, sociale sau de alt gen. Problema riscurilor informaționale şi minimizarea lor, an de an, devine tot mai profundă. În articolul dat este abordată o metodă de optimizare a sistemelor de management al securității informației, bazată pe teoria probabilităților.*

***Cuvinte cheie:*** *sistem, optimizare, securitatea informației, teoria probabilităților.*

## 1. Introducere

Informațiile sunt o resursă a organizației care, ca şi celelalte resurse importante de business, adaugă valoare organizației şi trebuie protejate ca atare. Securitatea informațiilor protejează informațiile organizației împotriva unei game variate de amenințări, în scopul asigurării continuității activității, minimizării daunelor posibile şi păstrării avantajului competitiv, profitabilității, şi chiar a legalității.

Un ajutor substanțial în crearea unui sistem de securitate informațională o pot acorda metodele de modelare matematică. În primul rînd, datorită lor e posibil de demonstrat managerilor că investirea finanțelor în sistemul de securitate informațională într-adevăr va economisi banii organizației (lipsa unei finanțări rezonabile în SSI constituie un impediment în dezvoltarea armonioasă a instituției). În al doilea rînd, în cazul insuficienței resurselor financiare pentru SSI, metodele matematice permit de a alege un complex optimal de măsuri de protecție, fiind posibilă modelarea - în ce măsură SSI creat va fi eficient în lupta împotriva celor mai răspîndite atacuri informaționale.

## 2. Optimizarea SMSI utilizînd teoria probabilităților

Modelarea matematică la optimizarea sistemelor de management a securității informației, reprezintă metode, în urma cărora pot fi obținute rezultate destul de eficiente . Voi face o analiză şi o descriere a unui model matematic de optimizare a sistemului de securitate informațională în cadrul unei organizații, bazat pe teoria probabilității. Să studiem un model care permite să se determine probabilitatea provocării daunelor sistemelor informaționale în cazul unui acces neautorizat (AN). Protecția contra AN se realizează printr-o succesiune de bariere, după trecerea cărora intrusul obține acces la resursele informaționale sau softul SIA.

Intrusul este în stare să pătrundă în sistem în condițiile cînd:

- el va poseda informații cu privire la sistemul de securitate (chiar şi întâmplător), fapt necesar pentru realizarea unei penetrări a sistemului de securitate;

- el va putea obține accesul la sistemele informaționale sau la resursele program pînă la momentul cînd sistemul de securitate va suferi metamorfoze (fapt care va crea noi obstacole în fața infractorului).

Să notăm cu $k_j$ numărul barierei, care constituie un impediment pentru accesarea infromației de tipul $j$. În cazul acesta probabilitatea că informația veridică $j$ în procesul de păstrare în baza de date nu va fi alterată ca urmare a AN la momentul livrării ei utilizatorului $P_{inf.j}$ se determină prin expresia (1):

$$P_{\inf .j} = 1 - \prod_{k_j=0}^{n} P_{nnj} \qquad (1)$$

unde $P_{nnj}$ – probabilitatea de penetrare a barierei;
$n$ – numărul de bariere a sistemului de securitate.

În cazul existenței unor delimitări în timp între elementele adiacente de modificare a parametrilor sistemului de securitate şi timpului de penetrare a sistemului de securitate, există probabilitatea de penetrare a barierei (2), ea fiind echivalentă cu:

$$P_{pentrare} = f\int_0^{\infty}\left(1 - F_{\text{mod}ificare}(t)\right)G_{bariera}(t)dt \tag{2}$$

unde $F_{modificare}$ - este funcția de distribuire a timpului între modificările adiacente a parametrilor sistemului de securitate;

$f$ - mărimea inversă timpului de aşteptare între modificările adiacente a parametrilor SI;

$G_{bariera}$ - funcția de distribuire a timpului de penetrare a barierei sistemului de securitate.

Reieşind din expresia respectivă, putem înscrie formula ce va determina probabilitatea penetrării sistemului întreg (3), adică penetrarea tuturor barierelor mecanismului de protecție:

$$P_{penetrare} = \prod_{k=1}^{n} f\int_0^{\infty}\left(1 - F_{\text{mod}ificare}(t)\right)G_{bariera}(t)dt \tag{3}$$

unde $k$ – numărul barierei din sistemul de securitate;

$n$ – numărul total de bariere a sistemului de securitate.

Sunt câteva cazuri pentru funcția de distribuire a timpului între modificările adiacente a parametrilor sistemului de securitate a barierei $F_{modificare}$:

Cazul 1. Parametrii sistemului de securitate se modifică într-un interval permanent de timp, adică $F_{modificare}(4)$ este determinat:

$$F_{\text{mod}ificare} = \begin{cases} 0, t < f^{-1} \\ 1, t \geq f^{-1} \end{cases} \tag{4}$$

Cazul 2. Intervalele de timp între modificările parametrilor adiacenți se determină întîmplător (5), spre exemplu cu ajutorul generatorului pseudoaleator al ordinii:

$$F_{\text{mod}ificare} = 1 - \exp(-ft) \tag{5}$$

Posibilele variante pentru funcția de distribuire a timpului pentru penetrarea barierei a sistemului de securitate $G_{bariera}(t)$:

Cazul 3. Timpul de penetrare a barierei sistemului de securitate este stabil (6):

$$G_{bariera}(t) = \begin{cases} 0, t \leq g^{-1} \\ 1, t > g^{-1} \end{cases} \tag{6}$$

Cazul 4. Să precăutăm cazul (7) cînd timpul pentru penetrarea de către atacator nu este cunoscut :

$$G_{bariera}(t) = 1 - \exp(-gt) \tag{7}$$

unde ***g*** – coeficientul de scară cu ajutorul căreia noi putem lua în considerație atît volumul operațiunilor complexe, cît şi nivelul de pregătire, precum şi de dotare tehnică a atacatorului.

Respectiv probabilitatea de penetrare a întregului sistem se va determina în baza formulelor următoare, în dependență de timpul de penetrare a protecției informației:

- în cazul cînd parametrii sistemului de securitate se modifică după intervale permanente de timp, iar timpul de penetrare a sistemei este permanent (8):

$$P_{penetrare} = \begin{cases} 0, f \geq g \\ 1 - f/g, f < g \end{cases} \quad (8)$$

- schimbul parametrilor se realizează după intervale egale de timp, iar tipul de penetrare a barierei nu este cunoscut (9):

$$P_{penetrare} = (1 - f/g)(1 - \exp(-g/f)) \quad (9)$$

- timpul între modificările parametrilor adiacenți se determină întîmplător, iar tipul de penetrare a barierei este permanent (10):

$$P_{penetrare} = \exp(-f/g) \quad (10)$$

- timpul între modificările parametrilor adiacenți se determină în mod întîmplător, timpul de penetrarea barierei nu este cunoscut (11):

$$P_{penetrare} = g/(g+f) \quad (11)$$

## 3. Concluzii

Crearea unui sistem de securitate informațională sigur este posibil, doar în cazul conexiunii active a elementelor clasice (elemente de soft, mijloace tehnice) precum şi a metodelor economice de protecție a informației. Conectarea eficientă a mecanismelor economice care permit anihilarea daunelor suferite de instituție (provocate sistemului informațional automatizat) este posibil doar în cazul prezenței unui SSI ce garantează cu o mai mare probabilitate integritatea informației. Anume în crearea unui SSI cît mai eficient din punct de vedere a rezistenței la potențialele atacuri informaționale, precum şi determinarea probabilității provocării daunelor de riscurile existente în condițiile unor resurse financiare limitate ne poate oferi complexul de modele pe care l-am prezentat in capitolul 2.

**Bibliografie**


1. Табаков А.Б., *Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков*// http://ej.kubagro.ru/
2. Девянин П. Н., *Модели безопасности компьютерных систем*: учеб. пособие для студ. высш. учеб. заведений, Москва, Издательский центр «Академия», 2005.
3. Баранов А. П., Борисенко Н. П., Зегжда П. Д., Корт С. С., Ростовцев А. Г. *Математические основы информационной безопасности*. Пособие, Орел, ВИПС, 1997.