УДК 004.9

Б.В.Дурняк, Т.М. Майба, УАД, м.Львів

МЕТОДИ ІНТЕРПРЕТАЦІЇ МОДЕЛЕЙ РИЗИКУ

Вступ

Модель ризику використовується для оцінки небезпеки, яка існує по відношенню до обєкту, чи процесу, який передбачається реалізовувати. Таким чином, уявлення про ризик, п своїй природі, представляє собою оцінку, яка є результатом прогнозування [1]. Прогнозування використовується в тих випадках, , коли не існує достатньо повної інформації про можливіпричини зміни величини ризику. Зацікавленість у змінах величини ризику $R(t)$ виникає тільки в тому випадку, коли передбачається, що ризик може збільшитися $R(t) \to N$. Другий фспект ризику полягає у визначенні границь зміни його величини та в інерпретації граничних змінних. Очевидно, що $[(R(t) > 0)\&(R(t) \neq 0)]$. Оскільки відсутність ризику, коли $R(t) = 0$ означає, що в принципі не може статися подія, що не передбачена технічними нормами на обєкт,чи процес, то таке твердження для технічних обєктів, чи процесів є не коректне, оскільки існує для останнього поняття ресурсу, яке інтерпретується, як деякий період часу, на пртязі якого використовується обєкт, або реалізується процес [2]. Оскільки, $R(t)$ не має обмежень в часі, то по закінченню інтервалу ΔT_i, який визначає ресурс, величина $R(t)$ приймає значення значення близьке до максимального, для відповідного обєкту. Більш того, з технічної точки зору, функціонування обєкту, чи процесу завжди може бути піддане дії зовнішніх негативних факторів, які можуть привести до порушень в процесі їх функціонування.Тому, нижня границя ресурсу $minR(t) = \delta > 0$, де δ – величина, що прямує до нуля. Верхня границя в різних випадках приймається рівною різним числам, які в кожному конкретному випадку обгрунтовуються. Ризик ніколи не може прямувати до нескінченості, оскільки в такій його інтерпретації не має сенсу. Це означає, що будь який обєкт, або процес не може функціонувати абсолютно точно у відповідності з технічними умовами.

Мета роботи - встановлення верхньої границі значення $R(t)$, тобто проведення аналізу параметрів процесу з ціллю визначення таких значень параметрів, при яких функціонування процесу приймається недопустимим.

Виклад основного матеріалу

Функціонування процесу приймається недопустимим, що можна описати наступним співвідношенням:

$$\{[\Pr(TO)] = F(P_1, \dots, P_n]\&[(P_1 > \delta_1) < \vee \dots \vee (P_n > \delta_n)]\} \to R(t) = max.$$

Виходячи з цього співвідношення, визначається величина $R(t) = \max\{N(P_i)\}$. Виходячи з приведеного, для встановлення масштабу вимірювання $R(t)$, необхідно провести аналіз величин відхилень парамерів

процесу від значень, або їх діапазонів, що визначені в документації на відповідні Pr_i. Такі відхилення, які будемо відносити до відхилень суттєвих, або значимих, необхідно співставити з відхиленнями параметрів продукту, які відповідними параметрами описуються. В даному випадку, продукт не обовязково повинен носити матеріальний характер, оскільи, це може бути та, чи інша послуга. На основі таких даних та на основі їх інтерпетації формуються значення величин $R(t)$, які представляються числами в діапазоні [0,1], але, при цьому, кожне число має інтерпретацію відповідного значення ризику. Таким чином, можна оримати ряд значень $R_i(t)$ у наступному вигляді:

$$Sz\big(R(t)\big) = \{R_1(t) * \dots * R_n(t)\},$$

де * означає спосіб конкатенації $R_i(t)$ і $R_j(t)$ між собою. Слід відмітити, що аргумент t, який використовується в $R_i(t)$ не має відношення до відповідної шкали $Sz\big(R(t)\big)$, а визначає момент реального часу процесу функціонування Pr(TO), в якому $R_i(t)$ приймає відповідне рішення. Для складних систем досить важко побудувати функціональну залежність між множиною змінних, що описують параметри Pr_i та загальним параметром $R_i(t)[ISU]$, який описує текучий стан системи. Тому Pr_i представляється у наступній формі:

$$Pr_i = F[pr_{i1}, \dots, pr_{in}],$$

де pr_{ij} – окремий підпроцес загального процесу Pr_i .

Для кожного pr_{ij} визначається своє значення $r_{ij}(t)$, яке описує величину ризику окремого підпроцесу. Тоді можна написати наступне співвідношення:

$$\{R_i(Pr_i)=[r_{i1}(pr_{i1}) * \dots * r_{in}(pr_{in})]\} \rightarrow \{f(r_{i1}, \dots, r_{in}) = R_i\big(t_j\big)\}.$$

Оскільки r_{ij} допускають інтерпретацію певного узагальнення параметрів окремих підсистем pr_{ij}, то легше сформувати функцію $f(r_{i1}, \dots, r_{in}) = R_i\big(t_j\big)$. Виходячи з приведеного співвідношення, можна стверджувати, що виличина ризику $R_i\big(t_j\big)$ співпадає з моментом часу, для якого величина ризику $R_i\big(t_j\big)$ визначається. Якщо продовжувати обчислення величини ризику в режимі реального часу на протязі інтервалу $\Delta T_i = \{t_{i+1}, \dots, t_{i+n}\}$, то отримаємо ряд значень $\{R(t_{i+1}), \dots, R(t_{i+n})\}$. Ці значення можна використовувати для апроксимації відповідної функції $R_i\big(t_j\big)$, завдяки чому стає можливим робити оцінку $R_i\big(t_{j+n-k}\big)$, де $k < n$. Цю процедуру можна інтерпретувати як прогнозування, якщо в режимі реального часу проводити модифікацію функції апроксимації:

$$R(t_i) = f_{Ap}(R_i, \dots, R_{i+n}). \quad (1)$$

Проблеми визначення величини ризику можна розвязувати на основі аналізу рівня безпеки системи. Інтерпретація величини ризику дозволяє уявлення про ризик повязати з інтерпретацією учявлень про безпеку системи (Bz_i). Такий інтерпретаційний звязок між $R(t_i)$ та Bz_i, який будемо позначати символом «⇒», дозволяє реалізувати конструктивні методи визначення $R(t_i)$.

На загальному рівні такий звязок описується наступним чином:

$$\{J[Bz_i] \Rightarrow J[R_i(t_i)]\} \Rightarrow \{R_i(t_i) = \Phi[Bz_i]\},$$

де $J[Bz_i] \rightarrow j(mt_i * Bz_i]$ і $J[R_i(t_i)] \rightarrow j[mt_i * R_i(t_i)]$, $\Phi[Bz_i]$ – визначає функціональну модель безпеки деякої системи. Безпосередньо з безпекою $Bz_i(ISU)$ повязані засоби, кожний з яких забезпечує протидію атаці відповідного типу A_i, яка активізується відповідною небезпекою. Такі конструктивні взаємозвязки між засобами захисту та $Bz_i(ISU)$ дозволяють прийняти той, або інший рівень безпеки $Bz_i(ISU) = \alpha$ на основі визначених даних про засоби захисту.

Як і у випадку з ризиком, $R(t_i)$, систему безпеки поділимо на цілий ряд підсистем, що орієнтовані на різні типи небезпек. Це дозволить більш просто визначати заданий рівень безпеки Bz_i, де Bz_i визначається, як:

$$Bz_i(ISU) = F(bz_i, \dots, bz_n)\ . \qquad (2)$$

Рівень безпеки в окремому функціональному підблоку значно простіше визначити на основі відповідних засобів захисту. В даному випадку, не розглядаються фактори внутрішнього характеру, які також можуть негативно впливати на процес Pr_i. Звязок між $R(t_i)$ та Bz_i, який використовується в роботі, грунтується на наступному твердженні.

Твердження 1. Між ризиком та рівнем безпеки існує обернено пропорціональна залежність:

$$R(t_i) = f(\alpha / Bz_i).$$

Нехай текстові описи $j[R(t)]$ і $j(Bz_i)$ є нормалізовані і мають спільний семантичний словник S_c, або $S_c \rightarrow j[R(t)]$ і $S_c \rightarrow j(Bz_i)$. Це означає, що всі $\{j[mt_i(R(t))] \in S_C\}\&\{j(mt_i(Bz_i)] \in S_C\} \rightarrow \{j[R(t)]\&j[Bz]\} \rightarrow S_C$. Будь який обєкт, чи процес pr_i описується окремими словами x_i, чи фразами φ_i, де $(x_i\&\varphi_i) \in S_C$. Доведення цього твердження має сенс в тому випадку, коли $(j(R(t)) \neq j(Bz)$. Текстовий опис $R(t)$ складається з компонент $mt_i(R_i)$, які можуть бути фразами $\varphi_i \in R(t)$. У випадку, коли в $j[R(t)]$ використовується слово x_i , то можна, для спрощення доведення, прийняти його, як фразу φ_i. Приймемо, що $(R(t)) \neq j(Bz)$, тоді можуть мати місце два випадки:

- Коли $\forall mt_i(R(t))\forall mt_i(Bz)[mt_iR(t) \neq mt_i(Br_i)]$,
- Коли $\forall mt_i(R(t))\forall mt_i(Bz)\exists mt_j(R(t))\exists mt_j(Bz)[mt_jR(t) = mt_j(Br_i)]$.

Розглянемо перший випадок. Виберемо в $j(R(t))$ елемент $mt_i(R(t)) = max\sigma^Z$, аналогічно, вибираємо з $j(Bz)$ елемент $mt_i(Bz) = max\sigma^Z$. Побудуємо вивід $mt_i(R(t))$ з S_C, або $mt_i(S_C) \rightarrow mt_i(R(t))$. Оскільки елементи з $j(R(t)) \in S_C$, то в S_C існують такі mt_i, з яких можна побудувати наступний вивід: $mt_i(S_C) \rightarrow mt_j(S_C) \rightarrow \dots \rightarrow mt_k(R(t))$. Можливість побудови такого виводу грунтується на тому, що $j(R(t))$ складається з елеменів, що належать S_C. Аналогічно розмірковуємо стосовно виводу $mt_r(S_C) \rightarrow mt_e(S_C) \rightarrow \dots \rightarrow mt_g(Bz_i)$. Доведемо, що у виводі $mt_i(S_C) \rightarrow mt_j(S_C) \rightarrow \dots \rightarrow mt_k(R(t))$ та $mt_r(S_C) \rightarrow mt_e(S_C) \rightarrow \dots \rightarrow mt_g(Bz_i)$ існують спільні елементи

$[mt_l(S_C) \in j(R(t))] \Leftrightarrow (S_C) \in j(Bz)$. Має місце співвідношення $[j(R(t))\&j(Bz)] \in \omega_i \in W_i$. Оскільки $R(t)$ і Bz_i є параметрами одного $\omega_i \in W_i$, то опис цих парамерів повинен вміщати спільні елементи. Виходячи з цього, можна прийняти, що має місце наступне співвідношення: $\{[\exists(mt_i \in R(t))\forall(mt_i(S_C))]\&[\exists(mt_j \in (Bz))\forall(mt_j(S_C))]\}\{[mt_j \in R(t)] \Leftrightarrow [mt_j \in (Bz)]\}$. Більш того, має місце наступне співвідношення: $\sigma^Z j(R(t)) = max\sigma^Z(mt_j \in \omega_i)$ і $\sigma^Z j(Bz_i) = max\sigma^Z(mt_j \in \omega_i)$. Але $j(R(t))\neg\Leftrightarrow j(Bz_i)$. Якщо семантичні значимості двох компонент S_C є одинаково значимі для $\omega_i \in W_i \subset S_C$, але мають різні інтерпретації, то врни повинні бути семантично суперечливі, або $\sigma^S[R(t), Bz_i] > \delta\sigma^S$, де $\delta\sigma^S$ – поріг допустимої семантичної суперечності. З іншого боку, $\{[j(R(t)) \in S_C]\&[j(Bz_i) \in S_C]\&[\sigma^S(R(t), Bz_i) > \delta\sigma^S\} \rightarrow [j(R(t)) = \neg j(Bz_i)]$. Оскільки $R(t)$ та Bz_i мають числові значення, то останні повинні бути обернено пропорціональні, або $R(t) = f(\alpha/Bz_i)$, що доводить твердження.

Для забезпечення ефективної протидії засобами SUB атакам, що можуть діяти на ISU, необхідно ввести структуру системи інтерпретації всіх компонент, які використовуються прни забезпеченні безпеки. Згідно з (1) і (2) існує можливість співвідносити олремі складові $Bz_i(ISU)$ із складовими $R(t_i)$. Оскільки $R(t_i)$ і, відповідно, $r_i(t_i)$ представляють оцінки рівня ризику, то не має сенсу величину ризику позначати тими, чи іншими числами, оскільки така оцінка повинна приводити до активізації дій, які могли б запобігти втратам, що визначені величиною $r_i(t_i)$. Це означає, що інтерпретація $r_i(t_i)$ і $R(t_i)$ в цілому, повинна описувати необхідні дії, до яких повинні вдаватися засоби захисту з SUB та повинні описувати події, до яких може привести дія небезпек, що визначають відповідний ризик $R(t_i)$. Це означає, що з інтерпретації величини ризику можна вивести інтерпретацію наслідків, до яких приводить дія факторів, що обумовлює встановлену величину ризику

В рамках даної роботи, фактори, що негативно діють на TP, або технічний обєкт (ТО) представляють собою атаки A_i, які формуються та ініціалізуються небезпеками, що існують в зовнішньому середовищі відповідного TP. В даному випадку, мова йде про інформаційну систему, під якою можна розуміти більш широку сутність, яка називається інформаційною технологією. Базовою послідовністю дієнеративних факторів, як уже зазначалось, є наступна послідовність:

$$Nb_i \rightarrow A_i \rightarrow Za_i \rightarrow Upr(SU_i),$$

де Upr – управляючий процес, що реалізується в ISU, SU_i – фрагмент управляючої системи ISU, який можна співставляти з окремим функціональним блоком Sb_i. Компонента Nb_i представляє собою деякий зовнішній процес, який ініціює атаку A_i, процес функціонування якої для системи є не відомим. Оскільки процес Nb_i формує та ініціює передачу атаки на обєкт, то його будемо називати процесом активізації атак GPr_i. По

відношенню до ISU, цей процес буде представляти собою сукупність описів відомих атак, що генеруються в GPr_i, а відповідні атаки будемо відносити до класу відомих атак, що можна записати у вигляді співвідношення:

$$GPr_i, \rightarrow APr_i(t) \rightarrow [APr_i(Za_i) \rightarrow Jt(A_i, t_i)] \rightarrow D(ISU),$$

де GPr_i – процес, який реалізується в рамках Nb_i , APr_i – прцеси, або один процес, що представляє собою атаку сформовану в GPr_i в момент t_i, $APr_i(Za_i)$ – взаємодія APr_i з загрозою Za_i , що є в ISU, $Jt(A_i, t_i)$ – інтруз, який сформувався в середовищі ISU в формі, яка відповідає середовищу. В даному випадку, такий $Jt(A_i, t_i)$ представляє собою програму, що відповідає A_i , $D(ISU)$ – дефект, або несправність, який може існувати необмежений час в неактивному стані в ISU, аьо може існувати короткий час в середовищі ISU, а також може сама по собі з часом зникнути. Процес APr_i на протязі своєго функціонування використовує загрозу Za_i , яка представляє собою додаткову умову для формування Jt_i. Це можна записати у вигляді: $(A_i \& Za_i) \rightarrow Jt_i(A_i, t_i)$.

Для протидії атакам з ціллю захисту ISU і, як наслідок, TPP в рамках засобів в SUB активізуються поцеси потидії негативним факторам. Активізація SUB реалізується в наступних випадках:

- в результаті активізації атак на обєкт,
- у випадку збільшення величини ризику,
- у звязку з реалізацією моніторингу засобів захисту.

Активізація SUB в результаті атакування обєкту зі сторони Nb_i здійснюється тільки в тому випадку, коли хочаби одна з атак проявить себе в системі. Це відбувається в результаті успішного виконання атакою хочаби одного кроку атаки. Завдяки успішному завершенню атаки зростає величина ризика $R(t_i)$. У випадку виявлення A_i система SUB активізує засоби діагностики Dz. Засоби Dzреалізують процес виявлення причин тих змін, до яких приводить успішні кроки атаки, або атака в цілому.

Активізація SUB , у звязку з реалізацією процесу моніторування, здійснюється у відповідності до реалізації стратегії захисту обєкту. Така стратегія грунтується на побудові моделі ризику, яка уже розглядалась і представляє собою:

$$R(t) = u + ct - \sum_{i=1}^{N_{\lambda(t)}} x_i, \qquad (3)$$

яка використовує уявлення про струмінь випадкових атак на ISU, який описується розподілом Пувсона з інтенсивністю λ. Величина обернена до λ є підставою, для визначення періоду моніторування. Приймемо, що цей період рівний деякій величині рівня $\Delta\tau$. Очевидно, що інтенсивність потоку може змінюватися. Якщо λ збільшується, то зменшується період моніторування. В процесі моніторування реалізується перевірка параметрів, що характеризують процес виконання атак. Прикладом таких параметрів може служити зміна величини доступної памяті, поява не ідентифікованих програмних фрагментів, зміна адрес переходів між штатними модулями програмного забезпечення ISU і т.д. Зміна величини $R(t)$, згідно з (3.3), може відбуватися

у звязку із збільшенням Za_i в процесі регламентного обслуговування SUB. В цьому випадку, $R(t)$ зменшується, що не приводить до активізації підсистеми моніторингу. В результаті здійснення ряду успішних атак, цей факт відображається в системі і $R(t)$ збільшується. Це приводить не стільки до активізації моніторингу, скільки до зменшення періоду моніторування, що опосереднено, приводить до збільшення активізації моніторування.

Розглянемо більш детально функціональний склад SUB, який приведено на рис.1.

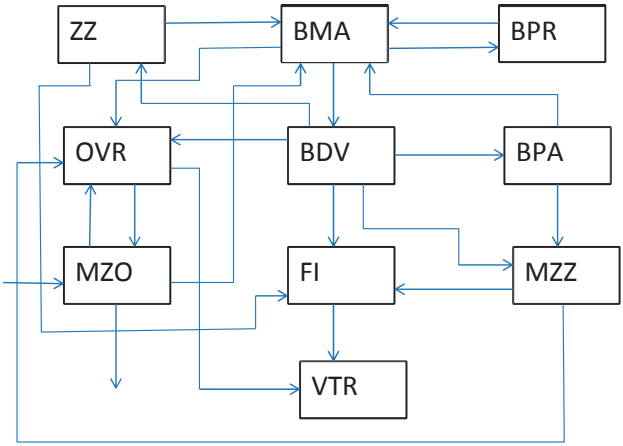

Рис. 1. Функціональна блок -схема SUB.

В SUB реалізуються наступні функціональні:

- моніторування обєкту захисту,
- діагностика,
- прогнозування атаки,
- протидія атаці,
- зменшення кількості загроз,
- обчислення ризику,
- модифікація засобів захисту,
- інтерпретація зміни величини ризику,
- інтерпретація взаємодії SUB і ISU,
- відображення стану системи.

На рисунку 3.1. використовуються наступні скорочення:

- BMA – блок моніторування атак,
- ZZ – блок елімінації загроз в обєкті захисту,
- BPR – блок прогнозування ризику,
- OVR – блок обчислення текучої величини ризику,
- BDV – блок діагностики результатів дії атак,
- BPA – блок протидії атаці,
- VZO – блок звязку SUB і системи ISU,

- FI – блок формування інтерпретаційного опису подій, що відбуваються в системі,

- MZZ –блок модифікації засобів захисту,

- VTR –блок відображення текучого стану системи захисту та величини ризику обєкту захисту.

На основі аналізу текучого стану обєкту захисту в модулі ZZ реалізуються процедури зменшення рівня загроз, що існують в системі. Оскільки загрозою є хактеристика одного з фрагментів системи, то мова не може йти про повну ліквідацію окремого Za_i, а тільки про зменшення величини значення відповідно параметру. Нприклад, якщо загроза характеризує міру перевірки пакету, який подається на вхід ISU, то зменшення величини загрози здійснюється шляхом розширення кількості параметрів пакету, які повинні перевірятися та інші.

Модель прогнозування величини ризику реалізує алгоритм прогнозування, який грунтується на використанні моделі величини ризику (3). Згідно з твердженням Крамера-Лундберга [3], яке формально записується у вигляді наступного співвідношення:

$$\lim_{u\to\infty\partial} e^{Ru}\psi(u) = \frac{\rho\mu}{k'(R)-c/\lambda}, \qquad (4)$$

де умова Крамера-Лунберга, якій задовільняє функція розподілу $F(x)$ ооописується наступним співвідношенням:

$$(\lambda/\mathrm{c})\int_0^\infty e^{Rx}[1-F(x)]dx = 1,$$

де R – показник Лунберга. В цьому випадку можна записати:

$$k(r) = \int_0^\infty e^{rz}dF(z) = 1\ .$$

Величина ρ у співвідношенні (4) є навантаженістю безпеки, $\mathrm{c} > \lambda/\mu$. З приведеного виникає приблизна рівність, для високого значення u, яке згідно з (3) описує початковий рівень безпеки, що забезпечується використанням впроваджених в SUB засобів захисту, яка формально описується наступним співвідношенням:

$$\psi(u) \approx (\rho\mu e^{-Ru})/(k'(R) - \frac{c}{\lambda}).$$

Ця функція називається функцією апроксимації Крамера-Лундберга і може використовуватися, при реалізації прогнозування зміни Bz_i і відповідно, зміни $R(t)$.

В рамках задачі прогнозування збільшення ризику, при ряді випадкових атак, функція розподілу яких відповідає геометричним розподілам з параметром $p = 1/(1+\rho)$, можна використовуати формулу Поллачека-Хінчина-Беекмана, яка описується співвідношенням з [4]:

$$\psi(u) = 1 - ((\rho/1)+\rho)\sum_{n=0}^{\infty}[H^{*n}(u)/(1+\rho)^n],$$

де $H^{*n}(u)$ – функція розподілу густини $f(x)$, яка рівна:

$$f(x) = \left(\frac{1}{\mu}\right)[1-F(x)], \quad x > 0.$$

Густина фунукції розподілу H^{*n} описується мпіввідношенням:

$$H^{*n}(x) = \int_0^\infty H^{*(n-1)}(x-1)dH(x),$$

де символ $H^{*(n)}(x)$ означає n – кратну згортку функції розподілу $H(x)$.

Приведені функціїрозподілу можуть використовуватися в якості основи, при побудові моделі прогнозування. По результатах такого прогнозування формується дисципліна моніторування стану системи захисту.

Функції діагностики, що реалізуються в рамках системи SUB дещо відрізняються від класичного підходу до розвязку задач діагностики [5]. В результаті моніторування система, що захищається, модуль діагностування отримує інформацію про виявлені аномалії в програмному середовищі. При цьому, задається функціональний блок, в якому виявлена аномалія та задається короткий опис атак, які найвірогідніше привели до виникнення відповідної аномалії. Функція діагностики блоку BDV орієнтовані на розвязок наступних задач виявлення причин аномалії і їх характеру:

- Задачі виявлення більш точних координат розміщення виявленої аномалії,
- Задачу відтворення траєкторії процесу функціонування інтруза , який сформований відповідною атакою,
- Задачу виникнення причин аномалії,
- Виявлення загрози, чку використала атаку для впровадження та формування відповідного інтруза,
- Визначення цілі, з якою відповідна атака діяла на систему захисту ISU,
- Визначення, чи ціль атаки досягнуто,
- Встановлення наслідків досягнення цілі виявленою атакою.

В залежності від рівня структуризації системи ISU, координати цілі аномалії, яку будемо позначати An_i , можна визначати різними способами, до яких віднесемо наступні типи способів визначення координат в програмному середовищі ISU.

Оскільки, програмне середовище є впорядкованим в рамках памяті, в якій воно розміщається, то її простір можна описати наступним чином:

- використовуючи ознаку, що вибирається на основі функціонального призначення тієї, чи іншої групи функцій, для реалізації яких призначені відповідні модулі програм,
- використовувати поділ простору памяті в основі якого лежить міра активності програм,
- розділяти простір памяті на частини, що призначені, для зберігання прогрпмних кодів та на частини памяті, які призначені, для зберігання кодів даних різного характеру та різного призначення,
- розділяти память на основі використання ідентифікаторів програмних модулів, які використовуються додатково в рамках системи ISU,
- порядком використання пограмних модулів та груп даних в рамках реалізації одного циклу функціонування системи управління TPP.

Висновки

Очевидно, що на всі ці критерії визначення просторових координат обєму памяті, в яких виявлено An_i, або $Jt(a_i)$, можна накладати адресну

систему, яка використовується у відповідній системі. В якості забезпечення прискорення пошуку $Jt(a_i)$, в середовищі ISU, можна використовуати деяку ієрархічну структуру, для вимірювання просторових координат. Перш за все, розділимо простір пошуку по типах памяті, оскільки відомо, що різні типи памяті мають різні системи доступу, що вимагає реалізації різних методів пошуку. Для спрощення аналізу, зупинимося на методі впровадження метрики, для оперативної памяті, яка в задежності від потреб системи може мати різний розмір, але в більшості випадків, використовує однотипні методи доступу до файлів програм та файлів даних.

1. *Половко А.М., Гуров С.В.* Надёжность технологических систем и техногенный риск. СПб.: Знание , 1998.
2. *Половко А.Н., Гиндин С.И.* Надёжность программного обеспечения в специализированных цифровых вычислительных компонентах. СПб.: ЦНИИ Румб, 1988.
3. *Фалин Г.Т.* Математический анализ рисков в страховании. М.: Российский юридический издательский дом. 1994.
4. *Ширяев А.Н.* Основы статистической финансовой математики. Теория. М.: Фазис. 1998.
5. *Рябинин И.А*. Надёжность и безопасность структурно-сложных систем. СПб.: Подитехника. 2000.

Поступила 28.9.2015р.

УДК 004.9+621.317+543

Л.С.Сікора, д.т.н., проф. НУ «Львівська Політехніка», Н.К.Лиса, к.т.н.,
Ю.Ю.Білак, к.ф-м.н., доц., Ужгородський національний університет

ІНФОРМАЦІЙНО-ЕНЕРГЕТИЧНА КОНЦЕПЦІЯ ТА БАЗОВІ МОДЕЛІ АКТИВІЗАЦІЇ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ НА ПІДСТАВІ ЛАЗЕРНОГО ФОТОННОГО ЗОНДУВАННЯ

Частина 1. Інформаційно–енергетична концепція

Анотація. Розглянуто нові методи активізації і контролю технологічних процесів та управління на підставі лазерних методів дистанційного зондування, обґрунтовано їх ефективність та якісний вплив на його хід.

Abstract. The paper considers new methods of activation and control of technological processes and management on the basis of laser remote sensing methods, substantiation of their efficiency and the qualitative impact on his move.

Ключові слова. Лазер, фотон, активізація, реакція, вимірювання, контроль.
Keywords*:* laser, photon, activation, control, signal.