УДК 004.9

МОДЕЛІ ВИЗНАЧЕННЯ ВЕЛИЧИНИ РИЗИКУ НА ОСНОВІ ВИКОРИСТАННЯ ЙМОВІРНІСНИХ ПІДХОДІВ

Б. В. Дурняк, Т. М. Майба

Українська академія друкарства,
вул. Підголоско, 19, Львів, 79020, Україна

У статті проаналізовано моделі визначення величини ризику на основі використання ймовірнісних підходів. Висвітлено різні аспекти інтерпретацій поняття ризику. Детально розглянуто фактори, від яких залежить рівень безпеки функціонування технологічного процесу поліграфії.

Ключові слова: *ризик, атака, об'єкт, загроза, безпека, засоби захисту.*

Постановка проблеми. Величини ризику є найпоширенішими параметрами під час оцінювання тих чи інших втрат. Якщо величина втрат не може бути визначена детерміновано у вигляді деякої числової величини, що допускає певну похибку, то для оцінювання таких втрат використовується деяка величина R, яка, за визначенням, є певним наближенням оцінки можливих втрат. Отже, ризик інтерпретується як оцінка певних втрат, яка їх визначає з точністю, що характеризується певним значенням ймовірності, що вказані втрати будуть.

Мета статті — проаналізувати різні моделі визначення величини ризику, використовуючи ймовірнісні підходи.

Виклад основного матеріалу дослідження. Для використання уявлення про ризик необхідно розглянути такі завдання: встановити причини виникнення випадкових факторів, що пов'язані з оцінками у вигляді ризику; встановити зв'язки ймовірних факторів з параметрами, які будуть оцінюватися величиною ризику R; розробити методи використання отриманих оцінок у формі ризику для реалізації процесів, які передбачається використовувати для впливу або управління факторами, що можуть бути залежними від оцінок, які можуть бути пов'язані з уявленнями про ризик.

Якщо йдеться про завдання захисту інформаційних систем управління технологічним процесом поліграфії (*TPP*), загрози втручання в такі системи розглядатимемо як випадкові події. В іншому разі було б відомо, коли таке втручання може відбутися і завдяки цьому була б можливість ефективніше йому протидіяти. Ще одним фактором, що в таких ситуаціях має ймовірнісний характер, є тип втручання або метод реалізації такого втручання. Щодо цього аспекту наявна інформація про відомі методи втручання, і їх кількість є множиною скінченною. Очевидно, що може виникнути певний тип втручання, який є невідомим, але це лише впливає на збільшення міри випадковості використання методів втручання в систему управління (*SU*) об'єктом типу *TPP*. Тому можна вважати, що фактори несанкціонованого втручання процес функціонування *SU(TPP)* мають ймовірнісний характер і можуть мати певні характеристики для відповідних ймовірнісних процесів [1–7].

Несанкціоноване втручання в *SU(TPP)*, за визначенням, реалізується з цілями негативного впливу на об'єкт. Негативний вплив на об'єкти, незалежно від конкретної цілі окремого фактора впливу, можна розглядати як зміну рівня безпеки функціонування *SU(TPP)*. Тому доцільно використовувати як параметр, що характеризує об'єкт і насамперед процес його функціонування, уявлення про безпеку даного об'єкта, яким є *SU(TPP)* і, як наслідок, сам процес *TPP*. Цей параметр будемо позначати літерою *B(SU)*, а в дужках вказуватимемо, безпеку чого в тому чи іншому випадку безпосередньо розглядатимемо. Зрозуміло, що в підсумку йдеться про безпеку *TPP* або загалом про систему *SU(TPP)*, що записується як *B*[*SU(TPP)*].

Очевидно, що використання уявлення про рівень безпеки функціонування *TPP* саме собою є необхідне. Але цього не достатньо для забезпечення оптимального процесу функціонування *TPP*. Рівень безпеки функціонування *TPP* повинен відповідати певним значенням, які не мусять бути максимальними. Необхідний рівень безпеки $B_i(SU)$ залежить від ряду факторів, до яких належать:

– атаки, що їх ініціюють небезпеки;
– значущість змін, що відбуваються в *TPP* у результаті дії успішних атак;
– вартість засобів захисту та вартість продукції;
– мобільність засобів захисту;
– ефективність системи, що взаємодіє з небезпекою, загрозами, атаками на об'єкт, що захищається.

Атаки, що ініціюються небезпеками і активізуються в середовищі засобів захисту, виникають лише тоді, коли в рамках небезпеки виявилось доцільно атакувати відповідний об'єкт. Якщо в рамках небезпеки немає підстав для активізації атак на *TPP*, то атак не буде. Це означає, що *SU(TPP)* не є достатньо важливим або, в певному сенсі, цінним, щоб зазнавати затрат на реалізацію атак на *TPP*. У цьому випадку необхідний рівень інформаційної безпеки досить низький, що оцінюється і, відповідно, низький рівень ризику *R(SU)*. Для однозначності використання термінології введемо визначення термінів, якими будемо послуговуватися у пропонованій праці.

Визначення 1. Небезпекою називатимемо деякий процес або об'єкт, який є зовнішнім стосовно об'єкта і функціонально може бути з об'єктом не пов'язаний. Позначатимемо небезпеку символом Nb_i.

Визначення 2. Загрозою для об'єкта, в цьому випадку для *SU(TPP)*, називатимемо характеристики *SU*, які можуть бути використані небезпекою для впровадження або ініціалізації в об'єкті атак. Загрозу будемо позначати символом Za_i.

Згідно із поширеною у сфері захисту інформаційних систем практикою такі характеристики називаються слабими місцями об'єкта, або *SU* [1]. Така термінологія не передбачає можливості відрізняти слабкі місця від місць неслабких і т. д.

Визначення 3. Атакою називається послідовність подій, що активізуються Nb_i завдяки використанню Za_i, які відбуваються в середовищі об'єкта і позначаються At_i.

Визначення 4. Безпекою об'єкта *SU(TPP)* будемо називати характеристику функціональних можливостей *SU(TPP)*, яка описує здатність системи захисту *(SZ(SU))* протидіяти атакам на *SU*, що ініційовані Nb_i.

Визначення 5. Ризиком називатимемо певним чином визначену міру величини, що характеризує безпеку функціонування об'єкта стосовно вимог, які обумовлюють певний спосіб функціонування об'єкта.

Поняття ризику в широкому розумінні означає оцінку небезпеки процесу або об'єкта, стосовно якого це поняття використовується. Важливим аспектом інтерпретацій поняття ризику є інтерпретація того, в чому полягають втрати, які оцінюються ризиком, та хто цих втрат зазнає. Цей аспект є досить важливим, бо ризик може бути пов'язаний з об'єктом, який зазнає втрат не безпосередньо, а опосереднено через засоби, які використовуються об'єктом для реалізації певних дій чи процесів. Щоб у роботі забезпечити однозначність інтерпретації відповідного поняття, вважатимемо, що деякий процес продукує певну продукцію, яка може мати певну вартість та вимірюватися певним обсягом. Споживачів продукту розглядати не будемо. На підставі цього приймемо такі положення:

Положення 1. Величину ризику будемо зіставляти зі зміною параметрів продукції або параметрів функціонування об'єкта чи суб'єкта, які, в результаті дії на процеси виробництва або на процеси діяльності негативних факторів, змінюють свої значення так, що відповідна зміна має негативну інтерпретацію.

Положення 2. Будь-який процес, або об'єкт, використовує засоби захисту, які забезпечують різні рівні безпеки.

Спираючись на наведені положення, вважатимемо, що небезпека для будь-якого об'єкта чи процесу в середовищі їх функціонування завжди існує. Це означає, що будь-який процес використовує засоби захисту. Природно припустити, що вартість засобів захисту є певною мірою еквівалентна вартості витрат, до яких призведе успішна дія небезпеки, що реалізується шляхом виконання атак. Можна прийняти, що величину ризику доцільно вимірювати у відносних величинах, які суттєво не залежать від різних одиниць вимірювання. Наприклад, якщо величину ризику вимірювати співвідношенням отриманих втрат у продукції (за рахунок зменшення її обсягів чи зниження її якості) до вартості використовуваних засобів захисту, то величина ризику буде величиною безрозмірною, або відносною. Формально це можна записати у вигляді співвідношення:

$$[R(TPP) \vee R(SU)] = (\sum^{m}_{(i=1)} \beta_i z_i) / (\sum^{n}_{(j=1)} \alpha_j x_j), \quad (1)$$

де x_j — кількість умовних одиниць бракованої продукції, α_j — її ціновий коефіцієнт, z_i — кількість засобів захисту, β_i — їх ціновий коефіцієнт. У цьому випадку приймається, що бракована продукція виникає лише в результаті дії на *SU(TPP)* атаки A_i, ініційованої N_b.

Наведений приклад підходу до визначення величини ризику дає змогу його визначати як факт, що уже стався. Здебільшого уявлення про ризик доцільно використовувати як деякий параметр, що дає змогу оцінити можливий ризик

іще до його настання, на відміну від випадку, наведеного у поданому співвідношенні (1). Можна прийняти, що *R(SU)* з формули (1) відображає один цикл роботи *TPP*, і тоді визначену величину *R(SU)* можна розглядати як можливу оцінку величини *R(SU)* для наступних циклів процесу функціонування *TPP*.

Розглянемо підхід, що дає можливість обчислити величину *R(SU)* для процесу *TPP*, який іще не почав функціонувати. Це зумовлює необхідність використання ймовірнісних методів обчислення величини ризику. Один з таких підходів може полягати у побудові функції апроксимації значень величини ризику.

Досить широко проблеми визначення величини ризику досліджувались у галузі функціонування страхових компаній. Для цих підходів характерне використання засобів теорії ймовірності, оскільки основні складники процесу функціонування страхових компаній не можуть бути описані детермінованими моделями [1, 2]. Аналогічна ситуація є у випадку функціонування системи захисту інформаційних систем, особливо інформаційних управляючих систем *(ISU)*. У випадку системи захисту *ISU* вхідними даними є фактори, що здійснюють зовнішню дію на *ISU*, які неможливо описати детермінованими засобами, оскільки ці дії визначаються небезпеками Nb_i, дію яких в часі неможливо описати детермінованими засобами. З точки зору можливості системи інформаційної безпеки *(SIB)*, яка є складовою *ISU* і орієнтовна на реалізацію захисту *ISU*, процес реалізації протидії атакам $A_i=f(Nb_i)$ засобами системи також не може бути описаний детермінованими моделями, тому що цей процес складається з виявлення атаки, її розпізнавання та реалізації деякого алгоритму протидії. Це формально можна описати таким співвідношенням:

$$V(A_i)\rightarrow R(A_i)\rightarrow P(A_i)\rightarrow[F(A_i)-\varepsilon(A_i)\rightarrow 0],$$

де $V(A_i)$ — виявлення атаки, $R(A_i)$ — розпізнавання атаки, $P(A_i)$ — протидія атаці, $F(A_i)$ — функція, що описує залишкову дію атаки на об'єкт, $\varepsilon(A_i)$ — ефективність дії атаки A_i на об'єкт *ISU*. Оскільки, за визначенням, тип можливої атаки та час, коли вона буде активізована, є параметрами випадковими, що визначаються природою функціонування Nb_i, то відповідні процеси повинні оцінюватися параметрами, що використовуються для опису випадкових подій. З огляду на те, що розпізнавання атаки не може бути повним, тому що Nb_i так формує A_i, щоб відповідна була розпізнаною або розпізнавальною хоча б частково, то реалізація процесу $P(A_i)$ також може мати в певних межах випадковий характер. Ефект дії атаки $\varepsilon(A_i)$ на *ISU*, враховуючи попередні фактори, має характер випадковий і допускає інтерпретацію вихідного процесу, що полягає у випуску продукції, певною мірою як процесу ймовірнісного.

Аналогія між страховою системою та системами безпеки *SIB* не обмежується тільки цілими процесами, а може бути розширена на окремі компоненти відповідних процесів. Це дає змогу адекватніше модифікувати відповідні моделі ризику, що використовуються для страхових компаній, до моделей ризику системи безпеки *SIB*. До таких компонент, у випадку страхових компаній, належать: капітал страхової компанії, аналогом її для *SIB* є система засобів захисту Za_i, кожний з яких орієнтований на окремий тип атак. Очевидно, що

необхідність в тій чи іншій кількості засобів визначається типами атак, які можуть діяти на *SIB*. Крім того, необхідно визначати ефективність атак, оскільки може виявитися, що та чи інша ефективність атаки $\varepsilon(A_i)$ може бути допустимою і, відповідно, засоби захисту можуть бути простішими. Детальніше ці особливості використання відомих ймовірнісних моделей для визначення оцінки ризику розглянемо в процесі аналізу відповідних моделей [3, 4].

Класичний процес ризику описується співвідношенням:

$$R(t) = u + ct - \sum_{j=1}^{N_\lambda(t)} x_j;\ t \geq 0, \qquad (2)$$

де u — початковий комплект засобів захисту; $c>0$ — інтенсивність розширення засобів захисту, яка визначається випадковим процесом появи атак, зокрема модифікованих атак на *ISU* та модифікацією і розширенням системи захисту на основі додаткових рішень про доцільність таких розширень, які загалом є випадковим процесом; x_i — втрати, які зумовлюються ефективністю атак на систему, оскільки така ефективність може бути задана дискретному просторі D; $N_\lambda(t)$ — відповідний процес Пуасона з інтенсивністю $\lambda>0$, де $\lambda=m/n$, який є незалежний від x_j, $j\geq 1$. Незалежність виникнення x_j і їх значень зумовлюється тим, що завдані ними втрати та ефективність їх дій можуть визначатися не тільки типами атак A_i на *ISU* , що призводять до виникнення аномалій, а й іншими факторами, що впливають на процес *TPP* загалом, які можуть не бути безпосередньо пов'язаними з Nb_i, що орієнтовані тільки на вплив щодо *ISU*. Процес ризику $R(t)$, описаний співвідношенням (2), піддається на інтервалі свого функціонування флуктуаціям, оскільки розміри систем захисту *SIB* не тільки розширяються, а можуть також зменшуватися через те, що неактивовані протягом певного часового інтервалу засоби захисту повинні елімінуватися з системи, що є випадковим процесом. Для розширення $R(t)$, використовується процес Кокса, який описується таким співвідношенням:

$$N(t)=N_1(\Lambda(t)),\ t\geq 0,$$

де $\Lambda(t)$ — процес керування процесом Кокса [5].

Приймемо, $\Lambda(t)=\Lambda t$,

де $\Lambda>0$ та $\mu(\Lambda)=a$, але для $\lambda>0, P(\Lambda>\lambda)>0$.

Якщо підзадачі $\psi(u,\lambda)$ як ймовірність виходу з ладу *TPP* або *ISU*, то ймовірність цього можна записати у вигляді:

$$\psi_1(u)=E\psi(u,\Lambda)-\int_0^\infty \psi(u,\Lambda)dP(\Lambda>\lambda).$$

Ця функція може бути описана так:

$$\psi_1(u)=E\psi(u,\Lambda):(\Lambda>c/a)+F(\Lambda\geq c/a)>0.$$

Природно записати вираз для процесу ризику $R(t)$ при $N(t),\ t\geq 0$ є процесом Кокса, що записується у вигляді:

$$R_2(t) = u + c\Lambda(t) - \sum_{j=1}^{N(t)} x_j;\ t\geq 0.$$

Ця модель враховує змінність процесу включення нових засобів захисту до складу *SIB*. Цей процес, що описує флуктуаційний процес ризику, називається узагальненим. Використовуючи уявлення про метрику Леві між функціями розподілу, яка описується співвідношенням:

$$L_1(X,Y)\equiv L_1(F_X,F_Y)=\forall(x\in R)\inf[h>0;F_Y(x-h)-h<F_X(Y)<F_Y(x+h)+h],$$

доводиться твердження про слабку збіжність, при $t\to\infty$, до розподіленої і випадкової величини Z. У нашому випадку існує такий фактор як взаємозв'язок між атаками та розширеннями *SIB* засобами z_i. У найпростішому випадку можна було б розглядати ситуацію, коли активізована атака A_i успішно була реалізована. Тоді, відповідно до даних *ISU* про наслідки успішної атаки та її профіль $\varphi_i(A_i)$, до складу *SIB* включається $z_i=\varphi^{-}(A_i)$, де функція $\varphi^{-}(A_i)$ описує послідовність протидії атаці A_i залежно від місця в траєкторії реалізації атаки $h(A_i,a_j)$, в якому відповідна атака була виявлена засобами $z_i=\psi(B_i,b_i)$. Змінна B_i описує необхідний процес протидії атаці A_i, який позначається $\psi(B_i,b_i)$. Згідно з твердженням про те, що одномірно розподілений, центрований, нормально узагальнений процес ризику $R_2(t)$ слабо збігається, при $t\to\infty$, до розподіленої випадкової величини Z, або:

$$\left\{\frac{\left[-R_2(t)-c(t)\right]}{D(t)}\right\}\to Z$$ тоді, коли $lim_{t\to\infty}\sup[(c(t))/(D^2(t)])=k^2<\infty$ та умов, що описуються співвідношенням $Z=k\sqrt{(a^2+\sigma^2)/[a-c]}-W+V$,

де W — випадкова величина з нормальним розподілом незалежно від V, то згідно з метрикою Леві має місце:

$$L_1\left\{\left[\frac{(a-c)\Lambda(t)-c(t)}{D(t)}\right]V(t)\right\}\to 0;\ t\to\infty.$$

Це означає, що розширення $R_2(t)$ кореляційними залежностями між $F_X(X)$ і $F_Y(Y)$ не призведе до порушення відповідної збіжності узагальненого ризику $R_2(t)$.

При реалізації та використанні *SIB* у вигляді застосування сукупності засобів захисту доцільно в ролі оцінок функціонування таких систем використовувати уявлення про вартість засобів захисту та вартість втрат, до яких можуть призвести успішно реалізовані атаки. Такий вартісний підхід відомий при дослідженні методів оцінювання величини ризику щодо систем інших типів [6]. Класичні методи розв'язання задач опису функціонування систем на основі оцінок ризику, що ґрунтуються на результатах Крамера–Лундерберга, прикладом яких є відповідна теорема, що формально описується так:

$$lim_{u\to\infty}e^{Ru}\psi(u)=\rho\mu/[K^{"}(R)-c/\lambda],$$

що ґрунтується на умові Крамера-Лундберга:

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

де R — показник Лундберга, $F(x)$ — функція розподілу атак на об'єкт захисту та на основі використання нерівності Лунсберга $\psi(u)\le e^{-Ru}$, ґрунтується на використанні математичних моделей, які не завжди відповідають дійсності. Тому важливим є вартісний підхід до розв'язання задач визначення оцінки ризику. В цьому випадку вважатимемо, що на початковій стадії маємо певну систему безпеки *SIB*, заповнену засобами захисту, які умовно мають відносну вартість U. Приймемо, що $N(t)$ —пуасонівський процес, що описує потік атак з інтенсивністю $\lambda>0$. Приймемо, що x_i — втрати, до яких призводить успішно реалізована атака, величина яких також є умовною. Тоді втрати $SU(TPP)$ за період $[0, t]$, можна описати співвідношенням:

$$S(t) = \sum_{i=1}^{N(t)} x_i - \alpha\lambda t\,,$$

де α — коефіцієнт узгодженості. Тоді $R(t)=u–S(t)$ інтерпретується як резерв вартості, якою володіє система незалежно від втрат за інтервал $[0, t]$. Величини $c_1(t,u)$ — затрати, що визначаються невикористаними засобами z_i, які потребують обслуговування та певних ресурсів для свого функціонування в пасивному режимі. Тоді $c_1(t,u)=c_1(t)>0$. Якщо $u<0$, то це означає, що *SIB* не заповнена до необхідного рівня і система приводить до часткових втрат. Приймемо, що $c_2(t)$ — вартість засобів z_i, якими необхідно доповнити *SIB*, щоб забезпечити необхідний рівень захисту. Тоді середні затрати $D(u)$ системи *SIB* визначаються для випадків, коли $u>0$, таким співвідношенням:

$$D(u)=u\int_0^T c_1(t)dt+\int_0^T c_2(t)E(s(t)–u)^+dt, \qquad (3)$$

де $x^+=\max\{x,0\}$, E — символ математичного очікування. Визначення мінімальних середніх сумарних затрат у (3). Приймемо, що x_j — неперервні, тому випадкова величина $S(t)$ має густину, яку позначимо $f_t(x)$. Оптимізація реалізується класичним чином на основі прирівняння до нуля похідної відповідних виразів. У цьому випадку можна записати:

$$\frac{dD(u)}{du} = \int_0^T c_2(t)P(S(t) \geq u)dt. \qquad (4)$$

Прирівнюючи (2.4) до нуля, отримаємо співвідношення:

$$\frac{1}{T}\int_0^T P(S(t) < u)dt = \delta, \qquad (5)$$

де $\delta=(c_2–c_1)/c_2$, приймається, що $c_1(t)=const=c_1$, $c_2(t)=const=c_2$. Тоді оптимальне початкове значення умовної вартості комплекту засобів захисту визначається розв'язанням рівняння (5). Щоб розв'язати це рівняння, треба знати розподіл випадкових величин x_i при $i\geq 1$. Прийнято функцію розподілу позначати $\Phi(x)$, а її густину — $\phi(x)$. Для спрощення розв'язку задачі в якості цих функцій приймемо перші два моменти $EX_i=m$ та $Dx_i=\sigma^2$. Приймемо $ES(t)=(m–a)t$, $DS(t)=\mu_2\lambda t$, де $Ex_i^2=\mu_2$, $Ex_i^3=\mu_3$. Згідно з [7], такі розв'язки являють собою наступні вирази. Для u_1 розв'язок рівняння (5) запишемо у вигляді:

$$\frac{1}{T}\int_0^T \Phi\left(\frac{u-m_1\lambda t}{\sqrt{\mu^2\lambda t}}\right)dt = \delta - \left(\frac{2L_3}{\sqrt{\lambda T}}\right),$$

де $L_3=c_0\mu_3/\mu_2^{3/2}$, c_0 — константа з нерівності Беррі-Естена. Для u_2 розв'язок рівняння (2.5) запишемо у вигляді:

$$\frac{1}{T}\int_0^T \Phi\left(\frac{u-m_1\lambda t}{\sqrt{\mu^2\lambda t}}\right)dt = \delta + \left(\frac{2L_3}{\sqrt{\lambda T}}\right),$$

де u_1 і u_2 — верхня і нижня границі u_0. Розв'язок ґрунтується на заміні невідомої підінтегральної функції на відому конструкцію зі збереженням монотонної залежності лівої частини (5).

Модель, розглянута вище, ґрунтується на використанні пуасонівського процесу, що описує потік атак, які реалізуються на *ISU*. Такий процес визначається характеристиками, що можуть використовуватися для досить адекватного опису потоку атак на об'єкт захисту. Інформаційні можливості такого процесу ґрунту-

ються на уявленнях про інформацію за Шеноном, яка формально описується таким співвідношенням:

$$I(AIB)=\log P(AiB)/P(A),$$

де A і B — події, що мають додатну ймовірність. Для випадку однієї події A, співвідношення для кількості інформації буде записане у вигляді:

$$I(A)=-\log P(A).$$

Розширенням уявлення про інформацію є уявлення про ентропію, що описується співвідношенням:

$$H(E)=EQ(E)=-\sum_{(i=1)}^{n} p_i \log p_i.$$

Зазвичай ентропія використовується як міра невизначеності деякого експерименту. Важлива властивість ентропії, яка використовується під час опису пуасонівських процесів, описується співвідношенням [5]:

$$H(X)=\lim_{(\delta\to 0)}[H(x_0)+\log \delta],$$

області D значень величини X.

Важливою аналітичною властивістю пуасонівського процесу є його асимптотична нормальність. Це означає, що в границі він може бути описаний нормальним розподілом випадкових подій, що формально описується співвідношенням:

$$P\left(\frac{N(t)-\lambda t}{\sqrt{\lambda t}} < x\right)\to \Phi(X), \text{ при } \lambda t\to\infty.$$

Висновки. Наведені характеристики та інформаційна інтерпретація характеристик розкладу Пуасона ілюструють доцільність його використання для опису потоку атак, що надходять на об’єкт, який необхідно захищати. Описаний підхід до побудови моделі ризику дає змогу обчислити величину ризику, наближаючи складові цієї моделі до засобів, що дозволяють достатньо адекватно описувати основні фактори, які зумовлюють можливість виникнення на об’єкті негативних результатів дії відповідних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бенинг И. У. Введение в математическую теорию риска / И. У. Бенинг, И. Ю. Королёв. — М. : МАКС-Пресс, 2000. — 435 с.
2. Артюхов С. И. Модель оптимального ценообразования, основанная на процессах риска со случайными премиями / С. И. Артюхов, О. А. Базюкина, В. Ю. Королёв, А. А. Кудрявцев // Системы и средства информатики. Специальный выпуск. — М. : ИПИРАН, 2005. — С. 205–222.
3. Бенинг И. У. Обобщённые процессы риска / И. У. Бенинг, И. Ю. Королёв. — М. : МАКС-Пресс, 2000. — 253 с.
4. Булинская У. В. Теория риска и перестрахования : Ч. 1. Упорядочение рисков / У. В. Булинская. — М.: Мех. мат. Фак. МГУ, 2001. — 215 с.
5. Грандел Я. Смешанные пуассоновские процессы / Я. Грандел // Обозрение промышленной и прикладной математики. Сер. «Финансовая и страховая математика. — 1998. — Т. 5, вып. 1. — С.44–65.
6. Кошаев Т. Р. Асимптотическое поведение обобщенных процесов риска, при возможности больших виплат / Т. Р. Кошаев, В. Ю. Королёв // Обозрение промышленной и прикладной математики. Сер. «Финансовая и страховая математика. — 2004. — Т. 11, вып. 1. — С. 57–71.

7. Ширяев А. И. Основы стохастической финансовой математики / А. И. Ширяев. — М. : Фазис, 1998. — 512 с.

REFERENCES

1. Bening S. (2000) *Vvedeniie v matematicheskuiu teoriiu riska* / Bening I. Korolëv I. M.: Max-press, 435 c. [in Russian]
2. Artuhov S. (2005), *Model optimalnogo cenoobrazovaniia, osnovannaia na processakh riska so sluchainymi premiiami*, K. Artûhov, A. Bazukina, Y. Korolëv, a. Kudryavtsev/ Systemy i sredstva informatiki. Special′nyi vypusk. M.: IPIRAN, S. 205–222. [in Russian]
3. Bening S. (2000). *Obobshchënnye processy riska*. M.: Max-press, 254 s. [in Russian]
4. U. Bulinskaia (2001). *Teoriia riska i perestrahovaniia*: part 1. Uporiadochenie riskov/V. Bulinskaia. M.: Fur. math. Fak. MSU, 215 p. [in Russian]
5. Grandel I. (1998), *Smeshannyie puassonovskie processy* / Obozrenie promyshlennoi i prikladnoi matematiki. Ser. «Finansovaia i strakhovaia matematika. T. 5, vyp. 1. s. 44–65. [in Russian]
6. Koshaev T. (2004). *Asimptoticheskoie povedenie obobshchennyh procesov riska, vozmozhnosti bol'shih vyplat* / T. Koshaev, y. Korolëv//Obozrenie promyshlennoi i prikladnoi matematiki. Ser. «Finansovaia i strakhovaia matematika. T. 11, vyp. 1. T 11, s. 57–71. [in Russian]
7. Shiriaiev A. (1998). *Osnovy stohasticheskoi finansovoi matematiki*, M.: Fazis, 512 c. [in Russian]

MODEL OF THE RISK MAGNITUDE DEFINITION BASED ON THE USE OF PROBABILISTIC APPROACHES

B. V. Durniak, T. M. Maiba

Ukrainian Academy of Printing,
19, Pidholosko St., Lviv, 79020, Ukraine
maiba@ukr.net

The article analyzes the model of the risk magnitude definition based on the use of probabilistic approaches. The paper considers different aspects of interpretation and the concept of risk. It is considered the factors that affect the safety level of the printing process functioning.

Keywords: *risk, attack, object, threat, security, safety.*

Стаття надійшла до редакції 27.03.2015.
Received 27.03.2015.