УДК 004.9

РОЗРОБЛЕННЯ АЛГОРИТМУ ФУНКЦІОНУВАННЯ МОДЕЛІ РИЗИКУ

Б. В. Дурняк, Т. М. Майба

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Модель ризику орієнтована на врахування випадкових факторів або недостатньо детермінованих, тому модель у загальному вигляді має неоднозначності. Одним із головних завдань алгоритму визначення величини ризику є мінімізація таких неоднозначностей. У вибраній моделі ризику алгоритм реалізує припущення та наявні в ній неоднозначності й залежно від сформованих вхідних умов здійснює коректну послідовність операцій, в результаті чого можна отримати адекватну оцінку ризику відповідного процесу функціонування технологічного процесу. Розглядаються зміни параметрів продукту, які не критичні для цілі його виготовлення, тобто належать до класу рівня безпеки, що відповідає зміні якості продукту.

Показано, що безпека, яка представляється ризиком, залежить від аварійних ситуацій, обумовлених неконтрольованими параметрами, що не відображені в рамках показників безпеки алгоритму визначення величини ризику, тому що ці параметри визначаються зовнішніми факторами, які можуть діяти на технологічний процес.

Ключові слова: *модель ризику, оцінка ризику, технологічний процес.*

Постановка проблеми. Потреба в розробленні алгоритмів функціонування окремої моделі ризику зумовлена тим, що вони формуються на основі різних підходів, характеризують ряд особливостей об’єкта функціонування, для якого передбачається визначати ризик, а також особливості інтерпретації окремих елементів моделі, містять інші особливості, які можуть відображати різні припущення, що закладаються під час формування моделі ризику [1]. Алгоритм, який реалізує у вибраній моделі ризику припущення та наявні в ній неоднозначності, повинен залежно від сформованих вхідних умов здійснювати коректну послідовність операцій, в результаті якої можна отримати достатньо адекватну оцінку ризику відповідного процесу функціонування, який може піддаватися впливу різних передбачуваних факторів.

Мета статті — побудувати алгоритм реалізації моделі ризику, який дає змогу зменшити міру невизначеності у відповідній моделі ризику, деталізувати міру загальності опису, яка використовується в рамках моделі, реалізувати механізм адаптації алгоритму до різних вхідних вимог, які відображають особливості задачі визначення величини ризику.

Виклад основного матеріалу дослідження. Існує цілий ряд додаткових факторів, врахування яких зумовлює потребу в деталізації елементів окремої моделі ризику. Загальність моделі ризику є природною за своєю суттю, оскільки здебільшого уявлення про ризик у різних випадках має різну інтерпретацію. Модель ризику орієнтована на врахування випадкових факторів або таких, інформація про які не є достатньо детермінованою, тому модель у своєму загальному вигляді має певні неоднозначності. Одним із головних завдань алгоритму визначення величини ризику є елімінація таких неоднозначностей. У рамках цих особливостей можна розглядати алгоритм визначення величини ризику як засіб, який повинен уточнити неоднозначності, щоб це не призвело, з одного боку, до суттєвого відхилення від реальних параметрів процесу, а з другого боку, забезпечило б можливість отримати достатньо адекватну оцінку величини ризику відповідного процесу. Дальшою проблемою, яку треба розв'язати, будуючи алгоритм обчислення ризику, є формування інтерпретації отриманої оцінки. Річ у тому, що ризик як окремий термін допускає різну інтерпретацію з погляду уявлень про функціонування досліджуваних процесів. Наприклад, однією з них може бути інтерпретація, яка полягає у визначенні ризику припинення функціонування самого процесу, стосовно якого встановлюється ризик, через дію на процес негативних факторів. Другим прикладом може бути інтерпретація, яка полягає у виході процесу функціонування за межі допустимого режиму і т. д. [2].

Іншим важливим завданням є мінімізація невизначеності, зумовлена тим, що елементи моделі являють собою ймовірнісні оцінки параметрів моделі або статистичні множини значень параметрів чи інші недетерміновані компоненти. Така мінімізація може бути досягнута за допомогою таких методів:

- заміна оцінкових параметрів на точні значення на основі положень або обмежень, що є допустимими для певних умов функціонування досліджуваного процесу;
- організація процесу, яка не призводить до наростання загальної похибки;
- використання вибраної інтерпретації оцінки ризику, яка відображає специфіку відповідної оцінки.

Алгоритм оцінки величини ризику (*AOR*) переважно орієнтований на діалог зі споживачем або, якщо результати його функціонування використовуються в системі, наприклад, для визначення рівня безпеки чи для інших цілей, то дані про величину ризику паралельно можуть видаватися користувачеві. Це означає, що *AOR* може бути розширений системою діалогу з користувачем, який в цьому випадку має можливість вводити уточнювальні дані або додаткові умови, які можна використати для модифікації алгоритму з метою уточнення результатів обчислення, що їх наводить *AOR*.

У випадку доповнення поняття ризику інтерпретаціями, які уточнюють, у чому полягає ризик, то залежно від інтерпретації величина ризику може мати різну точність. Очевидно, що таке уточнення являє собою найпоширенішу додаткову умову обчислення ризику. З конструктивного погляду в разі введення таких обмежень у моделі ризику можуть суттєво змінитися складові моделі або цілі фраг-

менти. Це означає, що *AOR*, по суті, є сукупністю алгоритмів, які реалізують різні версії моделей, що залежать від вхідних умов. Наприклад, якщо вхідною умовою є вимога обчислення ризику виникнення певної визначеної події, то в алгоритмі використовуються тільки ті дані й ті фрагменти моделі, які враховують фактори, що впливають на конкретну вибрану модель. Наприклад, якщо модель обчислення ризику являє собою співвідношення:

$$R(t) = U + ct - \sum_{j=1}^{N_\lambda(t)} x_j \text{, для } t \geq 0,$$

то початкова кількість засобів протидії факторам, що знижують рівень ризику, може вважатися мінімальною, тому що невідомо, якою буде ефективність λ впливу негативних факторів на систему в процесі виробництва товарів. Можлива ситуація, коли зовнішніх факторів негативного впливу не буде взагалі впродовж заданого періоду часу функціонування процесу.

Може бути запропонована така інтерпретація величини ризику алгоритму *AOR*, яка не потребує наведеної формули моделі ризику, а буде достатньо обчислити ймовірність виникнення деякої події, що залежить від різних відомих негативних факторів. Наприклад, визначаючи величину ризику, може виявитися достатньо обчислити ймовірність вимкнення живлення, виходу з ладу функціонально важливої компоненти технологічного процесу чи ймовірність інших подій, які впливають на *DTP*, порушуючи виробництво.

Оскільки визначувана інтерпретація оцінки ризику є ключовою для вибору методів обчислення $R(t)$, то для адаптації методів обчислення ризику до особливостей, обумовлених окремою задачею, яку розв'язує система управління, необхідно детальніше зупинитися на різних типах ризику, можливих у *TPP*. До таких типів ризику можна зарахувати:

- ризик того, що продукт, який виготовляється в *TPP*, не буде виготовлений. Такий ризик будемо називати глобальним (позначатимемо його *Rg*);
- ризик відмов у *TPP*, які є критичними (*Rv*);
- ризик відмови окремих фрагментів *TPP*, що призводить до порушення умов і термінів виготовлення продукції (Ru^i);
- ризик зниження якості продукції (*Rj*), яка може бути випущена в рамках *TPP*, що пов'язано зі змінами значень параметрів, які безпосередньо впливають на якість продукції, та інші типи ризику.

Наведені типи ризику ілюструють тісну залежність текстової інтерпретації кожного з ризиків $j(R_i)$ з предметною галуззю інтерпретації, до якої належить *TPP*.

Якщо *TPP* являє собою засіб, який є досить універсальним, то відповідне $W_i(TPP)$ буде великим за розмірами своїх компонент. Важливою особливістю параметра ризику $R(TPP)$ є його тісний зв'язок з ціллю або рядом цілей, що зумовлюють його використання. Отож, визначення типів ризику R_i можна будувати на основі аналізу цілі, безпосередньо пов'язаної з даними *TPP*. Підвищення універсальності *TPP* або розширення $W_i(TPP)$, що можна уточнювати, збільшує кількість цілей застосування *TPP* і, відповідно, кількість типів ризику. У зв'язку з цим уважатимемо, що в рамках *TPP* можливі такі ризики:

– ризик невиготовлення продукції (*Rg*);
– ризик відмови процесу функціонування технологічного обладнання (*Rv*);
– ризик зниження якості продукції, що виробляється відповідними $TPP(R_j)$.

Алгоритм обчислення величини ризику повинен забезпечувати обчислення необхідних типів ризику, які встановлює користувач відповідно до можливостей *TPP*, що описується в рамках $W_i(TPP)$. Величину ризику можна визначати на основі описаних нижче підходів.

Перший підхід полягає у безпосередньому визначенні ризику на основі даних, які характеризують ймовірність виникнення аномалій, що призводять до виникнення ризиків різних типів. Для спрощення обчислення ризику весь технологічний процес поділяється на окремі функціональні компоненти, і в цьому випадку ризик обчислюється для кожного фрагмента Pr_i окремо. За окремими ризиками $R(Pr_i)$ обчислюється загальний ризик.

Другий підхід до обчислення ризику ґрунтується на існуванні зв'язку між рівнем безпеки та ризиком. Оскільки рівень безпеки обчислюється простіше на основі використання конструктивних залежностей між аномаліями різних типів і причинами їх виникнення, то рівень безпеки може бути обчислений більш адекватно до реального стану *TPP*.

Беручи до уваги викладене, будуватимемо алгоритм *AOR*, використовуючи другий підхід. У цьому випадку типи ризиків *Rv*, *Rg*, *Ru*, *Rj* допускають відповідні інтерпретації в поняттях різних типів і рівнів безпеки. Ризик типу *Rg* відповідає загальному рівню безпеки системи, який позначатимемо Bz_g. Ризик типу *Rv* буде відповідати рівню безпеки Bz_v, який визначатиметься на основі даних про надійність відповідних фрагментів $Pr_i \in TPP$. Кожний із таких фрагментів складається з апаратурної частини, надійність якої являє собою паспортні дані на відповідний технологічний засіб. Тому стосовно апаратурних засобів відповідна складова рівня безпеки є відомою. Цю складову будемо позначати в $Bp \in Bv$. Крім апаратурної складової до фрагмента $Pr_i \in TPP$ належать програмні засоби, які здійснюють керування відповідним засобом і синхронізують його з іншими складовими в рамках *ISU*, що обслуговує весь *TPP*. Цю складову позначатимемо $b_{pr} \in B_v$. Надійність програмного забезпечення, орієнтованого на розв'язування певних задач керування, може бути розрахована за відомими моделями надійності програмних засобів [3, 4]. Цю складову рівня безпеки, що входить у b_m, позначатимемо символом $b_m(PO) = b_{PO}$. Крім цієї складової, в b_m входить складова безпеки, яка визначається зовнішнім втручанням у роботу *ISU* або зовнішніми факторами, які називаються атаками на *ISU*. Такі зовнішні фактори досить широко досліджуються у зв'язку з вивченням системи захисту від атак на системи типу *ISU* та методів забезпечення безпеки інформаційних систем стосовно атак [5]. Цю складову будемо позначати $b_m(At_i)$. Тоді можна записати:

$$b_m = f[b_m(PO), b_m(At_i)].$$

Ризик типу R_u, який залежить від подій, що полягають у порушенні умов виробництва продукції, але не є критичними для процесу продукування, можна зарахувати до безпеки, яка характеризує можливість виникнення змін у процесі, що

порушують умови виконання замовлення, яке реалізується в *TPP*. До таких умов належать такі фактори:

- термін виконання замовлення;
- зміни параметрів продукту, що не є критичним для цілі виготовлення продукту;
- зміна вартості продукту;
- відмова замовника від продукту в період його виготовлення;
- поява неконтрольованих відхилень у параметрах продукту в процесі його виробництва.

Зміну терміну виконання замовлення будемо пов'язувати лише з подіями, зумовленими змінами в *TPP*. Такі зміни полягають у виникненні тимчасових відмов у засобах *TPP*, що приводить до появи складової, яку позначатимемо *bvp* і яка є складовою рівня безпеки *Bv*(*bvp* ∈ *Bv*). Важливою складовою рівня безпеки *Bu* є зміни в процесі функціонування *TPP*, зумовлені людським фактором. Цю складову *Bu* будемо позначати *bLf* . Рівень цієї небезпеки визначатимемо на основі таких факторів. Здебільшого він пов'язаний із соціальними та психологічними аспектами, що характеризують персонал обслуги. Тому цей аспект оцінки *bLf* аналізувати не будемо. Відомо, що рівень автоматизації управління процесом *TPP* визначає міру участі персоналу обслуги в реалізації процесу функціонування *TPP*. Такий рівень можна визначити на основі аналізу кількості керівних дій персоналу обслуги з урахуванням важливості відповідної дії на *TPP* або впливу такої дії на отримання кінцевого продукту. Ці дії позначатимемо символом *dLi*, а *αd* буде означати значущість такої дії для *TPP*. З другого боку, в *TPP* існує потреба виконання керівних дій, зумовлена технічними умовами на відповідний тип обладнання. При включенні деякої одиниці обладнання в *TPP* відповідні керівні дії можна реалізувати на основі автоматизації управління *TPP* загалом. Сучасне обладнання переважно передбачає таку автоматизацію. Таким чином, можна визначити загальну кількість керівних дій, необхідну для використання відповідного пристрою в *TPP*. В цьому випадку рівень безпеки функціонування окремого пристрою в *TPP*, який визначається впливом *bLi*, можна визначити таким співвідношенням

$$b_{Lf} = \left(\sum_{i=1}^{k} e_i \alpha_{di} d_{Li} \right) / d_{Ni},$$

де d_{Ni} — загальна кількість керівних дій, яку треба реалізувати стосовно пристрою в процесі його функціонування в складі *TPP*.

Зміни параметрів продукту, що не є критичні для цілі його виготовлення, належатимуть до класу рівня безпеки, який зіставляється з ризиком типу R_j, що відповідає зміні якості продукту. Зміна вартості продукту може бути ініційована виробником, оскільки замовник визначає ціну під час укладення договору на виготовлення товару. Зміна вартості виробів, яка виникає зі сторони виробника, зумовлена потребою зміни запланованих матеріалів на дорожчі або зміною цін на ринку відповідних матеріалів. Виникнення небезпеки цього типу буде належати до людських факторів організаційного характеру і позначатимемо таку компоненту рівня безпеки b_{Lo}. Її величину будемо задавати на основі статистичних даних, які

відображають виникнення відповідних ситуацій в минулому. На період одного циклу експлуатації *TPP*, визначеного періодом виготовлення замовлення, параметр b_{Lo} вважатимемо сталим. Очевидно, що b_{Lo}= 0, якщо всі необхідні матеріали для виконання замовлення вже є у виробника.

Відмова замовника від замовлення під час реалізації процесу *TPP* його виготовлення переважно є передбачена й обумовлена в умові щодо замовлення так, щоб виробник не зазнав у зв'язку з цим втрат. Тому цю складову в складі B_u розглядати не будемо. Отже, рівень безпеки B_u, який зіставляється з ризиком R_u, визначатиметься таким співвідношенням:

$$B_u = b_{Lf} + b_{Lo}.$$

Ризик зниження параметрів якості продукції будемо зіставляти з підвищенням рівня безпеки отримання продукту із заданими параметрами. Якщо задані параметри продукту $\{p_1, p_2, \ldots, p_k\}$ повністю відповідають параметрам продукту, який виготовлено $\{p^*_1, \ldots, p^*_k\}$, то величина ризику для цього типу реалізації *TPP* дорівнює нулю, або величина безпеки забезпечення необхідних параметрів якості дорівнює одиниці. Забезпечення певних параметрів для продукту Q_i в рамках *TPP* реалізується за допомогою контролю параметрів *TPP*. Якщо такий контроль параметрів не є повним з погляду забезпечення необхідних показників якості продуктів виробництва, то рівень безпеки можна описати таким співвідношенням:

$$B_i = \left(\sum_{i=1}^{k} \beta_i \cdot p_{ji} \right) / P,$$

де β_i — коефіцієнт значущості параметра p_{ji}, p_N — сума всіх параметрів, які підлягають регулюванню для реалізації процесу *TPP*, p_{ji} — параметри, що регулюються в процесі реалізації персоналом обслуги.

На рисунку зображена функціональна схема реалізації алгоритму оцінки загального рівня безпеки. Використано такі позначення:

- N_1, N_2, N_3, N_4 — індикатори аналізу всіх рівнів безпеки;
- *BG* — перевірка, чи є параметри для безпеки типу *BG*;
- *FBG* — формування значення рівня безпеки *BG*;
- *BV* — перевірка, чи є параметри безпеки типу *BV*;
- *WPBV* — вибір параметрів безпеки *BV*;
- *NA* — перевірка, чи параметри, що стосуються апаратури;
- *NABA* — формування складової параметра апаратури;
- *NP* — перевірка, чи є складові параметри програм;
- *NPBP* — формування складових параметрів для програм;
- *FSPB* — формування сумарного параметра *BV*;
- *FB* — перевірка, чи змінився параметр безпеки *BV*;
- *PB*01 — формування величини зміни параметра *BV*;
- *BU* — перевірка, чи є параметр безпеки типу *BU*;
- *WPBU* — вибір параметрів для безпеки *BU*;
- *LF* — перевірка, чи є складовий параметр людського фактора;
- *WLF* — формування параметра людського фактора;
- *LO* — перевірка, чи є складовий параметр організації процесу;

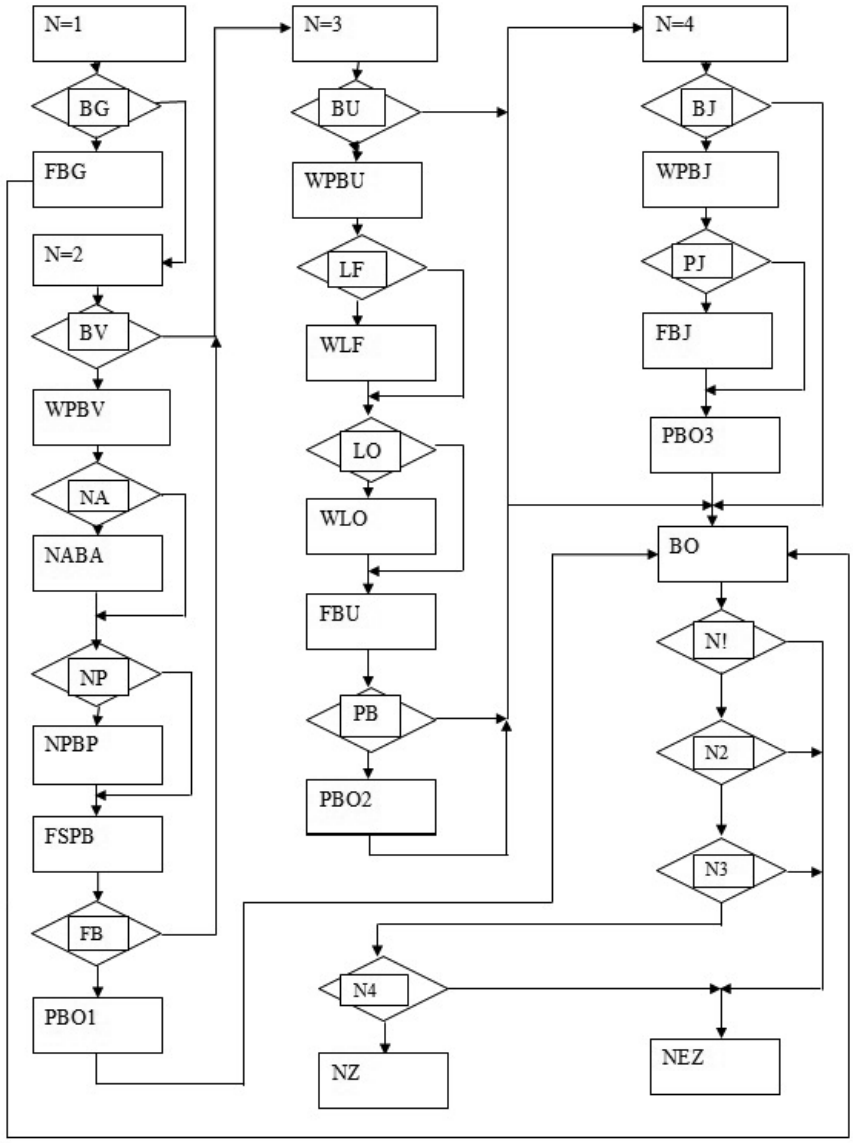

Рис. Функціональна схема

- *WLO* — формування параметра організації процесу;
- *FBU* — формування загального параметра *BU*;
- *PB* — чи значення параметра *BU* змінилося;
- *BB*02 — формування величини зміни параметра *BU*;
- *BJ* — перевірка, чи є параметри типу *BJ*;
- *WPBJ* — вибір параметра типу *BJ*;
- *PJ* — чи є параметри якості продукту;
- *FBJ* — формування параметрів якості продукту;
- *PB*03 — формування величини зміни параметрів *BJ*;

– *BO* — формування загальної величини безпеки;
– *N*1 — перевірка, чи були проаналізовані параметри *BG*;
– *N*2 — перевірка, чи були проаналізовані параметри *BUV*;
– *N*3 — перевірка, чи були проаналізовані параметри *BV*;
– *N*4 — перевірка, чи були проаналізовані параметри *BJ*;
– *NZ* — коректне завершення алгоритму;
– *NEZ* — некоректне завершення алгоритму.

Висновки. Безпека, що представляється ризиком R_g, залежить від аварійних ситуацій, обумовлених параметрами, які не контролюються в рамках показників безпеки типу B_v, B_u та B_j тому, що ці параметри визначаються зовнішніми факторами, які можуть діяти на процеси *TPP* загалом. До таких факторів належать техногенні фактори, зумовлені змінами в зовнішньому середовищі, економічні та соціальні фактори. Вплив цих факторів можна врахувати лише на основі використання моделей прогнозування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лашев Т. Р. Математические методы оценки оптимальных параметров процесов риска / Т. Р. Лашев, В. Ю. Королёв, С. А. Шаргин // Системы и средства информатики. — М. : ИПИ РАН, 2002. — С. 127–141;
2. Прохоров Ю. В. Асимптотические методы математической теории риска, основанные на смешанных пуассоновских моделях / Ю. В. Прохоров, В. Ю. Королёв, В. В. Бенинг // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. Специальный выпуск. — 2005. — С. 94–112.
3. Рябинин И. А. Надёжность и безопасность структурно-надёжных систем / И. А. Рябинин. — СПб. : Политехника, 2000. — 347 с.
4. Надёжность технических систем / Под ред. Е. В. Сучака, Н. В. Василенко. — Красноярск : МГП «Раско», 2001. — 600 с.
5. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. — СПБ. : БХВ-Петербург, 2001. — 642 с.

REFERENCES

1. Lashev, T. R., Korolyov, V. Yu., & Shargin, S. A. (2002). Matematicheskie metody otsenki optimalnyih parametrov protsesov riska. Sistemyi i sredstva informatiki. Moscow: IPI RAN, 127–141(in Russian).
2. Prohorov, Yu. V., Korolyov, V. Yu., & Bening, V. V. (2005). Asimptoticheskie metody matematicheskoy teorii riska, osnovannyie na smeshannyih puassonovskih modelyah. Vestnik Moskovskogo universiteta. Seriya 15: Vyichislitelnaya matematika i kibernetika. Spetsialnyi vypusk, 94–112 (in Russian).
3. Ryabinin, I. A. (2000). Nadyozhnost i bezopasnost strukturno-nadYozhnyih sistem. Sankt-Peterburg: Politehnika (in Russian).
4. Suchak, E. V., & Vasilenko, N. V. (Eds.). (2001). Nadyozhnost tehnicheskih sistem. Krasnoyarsk: MGP «Rasko» (in Russian).
5. Lukatskiy, A. V. (2001). Obnaruzhenie atak. Sankt-Peterburg: BHV-Peterburg (in Russian).

DEVELOPMENT OF FUNCTIONING ALGORITHM OF A RISK MODEL

B. V. Durniak, T. M. Maiba

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine

The risk model is focused on random or not determined enough factors, so the model is ambiguous in general. One of the main objectives of the algorithm for determining the risk value is to minimize these ambiguities. In the selected risk model the algorithm implements the assumptions and existing ambiguity in it and depending on the prevailing conditions inputs the correct sequence of operations, resulting with an adequate risk assessment of the relevant process of the technological operation. We consider changing the parameters of the product that are not critical for purposes of manufacturing, which means they belong to the class of security level appropriate to changes of the product quality.

It has been shown that the security that appears as a risk depends on accidents caused by uncontrollable parameters that are not reflected within the security parameters of the algorithm of the risk determination because these parameters are determined by external factors that may operate in the technological process.

Keywords: *risk model, risk assessment, technological process.*

Стаття надійшла до редакції 15.06.2016.
Received 15.06.2016.