УДК 004.9

СИНТЕЗ МОДЕЛЕЙ РИЗИКУ З ІНФОРМАЦІЙНИМИ КОМПОНЕНТАМИ

Б. В. Дурняк, Т. М. Майба
Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Розглянуто процеси синтезу моделі ризику з інформаційними компонентами, що безпосередньо впливають на величину ризику. Описано фактори, які можуть суттєво впливати на величину ризику. Висвітлено можливості реалізації процесу управління технологічними процесами на основі виконання τ-функції, які оперують таблицями відомих множин значень вхідних параметрів, відомих множин проміжних значень параметрів функцій та відомих множин значень аргументів.

Ключові слова: *модель ризику, процеси синтезу, атаки, загрози.*

Постановка проблеми. Синтез моделей ризику з інформаційними компонентами уможливлює розширення відповідних моделей інтерпретаційними описами, що дає змогу в рамках окремої моделі враховувати більше факторів, які можуть суттєво впливати на величину ризику. Інформація, що стосується моделей ризику, є багатоплановою, оскільки поняття ризику є досить широке і для того, щоб у міру можливості в рамках параметра ризику враховувати всі фактори, які на нього впливають, необхідно при його визначенні та обчисленні брати до уваги всі пов'язані з ним аспекти.

Мета статті — синтез інформаційного доповнення процесів, які використовуються під час обчислення ризику.

Виклад основного матеріалу дослідження. До окремих факторів, які складно конструктивно включити до математичної моделі ризику, можна віднести такі:

- інформація про основні процеси, стосовно яких визначається величина ризику, та їх негативний вплив;
- інформація про засоби, які орієнтовані на те, щоб рівень відповідного ризику підтримувати та не допускати його зниження чи зростання в процесі реалізації основних функцій об'єкта, стосовно якого обчислюється величина ризику;
- інформація про нерегулярні фактори, які діють на об'єкт, збільшуючи величину ризику;
- інформація про випадкові фактори, що можуть своєю дією на основний процес спричиняти збільшення величини ризику;
- інформація про цілі функціонування процесу, на досягнення яких невідповідний рівень ризику може негативно впливати;
- інформація про інтерпретацію ризику в предметній області процесів, для характеристики яких він використовується і які можуть зумовлювати ситуації,

в яких ризик не тільки зменшується, але й збільшується, оскільки його зменшення може призводити до затрат, які не будуть обґрунтованими;

– однією з важливих компонент, що стосуються аналізу ризику, є інформація про природу причин, які безпосередньо зумовлюють відповідний ризик, оскільки можлива ситуація, коли такі причини впливу на величину ризику мало пов'язані з природою процесу, щодо якого відповідний ризик визначається та враховується;
– у зв'язку з тим, що, з одного боку, ризик є досить широким поняттям, а з другого — його необхідно зіставляти з основними процесами, стосовно яких цей ризик визначається, то в кожному випадку ризик треба визначати таким чином, щоб він найбільшою мірою стосувався відповідного процесу;
– на основі додаткової інформації про об'єкти ризику можливо оптимізувати уявлення про ризик, пов'язаний з певним процесом, таким способом, щоб не поширювати його поза межами, в рамках яких величина ризику досліджується.

Обмеження факторів, що визначають ризик процесами, до яких передбачається їх застосовувати, ґрунтується на описі безпосереднього процесу, який досліджується. У цьому випадку таким процесом є сукупність підпроцесів, що реалізують управління окремими компонентами *TPP*. З цього погляду одним із аспектів ризику є ризик того, що значення параметрів технологічного процесу вийдуть за допустимі межі, що призведе до порушення процесу управління. У цій роботі не розглядатимемо всі можливі причини таких змін, а тільки причини, зумовлені дією зовнішніх факторів, що негативно впливають на управляючі процеси. Вплив таких негативних факторів може проявлятися у вигляді реалізації атак A_i на систему управління *ISU* технологічним процесом [2, 3]. Причинами виникнення зовнішніх атак є небезпеки Nb_i, які існують у зовнішньому середовищі незалежно від того, чи є та чи інша система функціонування в деякому середовищі, чи її не має. Для захисту від негативної дії на *ISU* зовнішніх факторів використовується система захисту або система управління безпекою відповідної *ISU*. Враховуючи функціональну орієнтацію системи управління безпекою *SUB*, можна стверджувати, що остання повинна забезпечувати певний рівень безпеки системи *ISU*. Якщо безпеку розглядати як фактор, який запобігає недопустимим відхиленням значень технологічних параметрів, то рівень безпеки Bz_i можна розглядати як величину, пов'язану з величиною ризику $R(t_f)$ обернено пропорційною залежністю. Тому першою компонентою синтезу засобів, що зумовлюють можливість зміни ризику з компонентами, які з погляду моделі ризику допускають таку інтерпретацію, як компонента інформаційного характеру, є синтез системи *ISU* як інформаційної складової для моделі ризику з системою *SUB* як системою, що безпосередньо впливає на величину ризику. Отож можна стверджувати, що *SUB* є однією з компонент, що забезпечує можливість функціонування моделі ризику. На рис. 1 зображено синтез функціональних блок-схем системи управління як об'єкта, стосовно якого визначається величина ризику $R(t_f)$, та системи *SUB*, яка впливає на величину ризику $R(t_f)$, хоча за своєю природою не є безпосередньою реалізацією моделі ризику $R(t_f)$.

У пропонованій праці процеси синтезу моделі ризику з інформаційними компонентами, що безпосередньо впливають на величину $R(t_i)$, розглядаємо як процес, який складається з ряду компонент або окремих процесів синтезу різних інформаційних компонент зі складовими, що допускають свою інтерпретацію як складові моделі ризику. Це зумовлено тим, що, з одного боку, уявлення про ризик є досить широке, а з другого боку, для забезпечення конструктивного синтезу моделі ризику з інформаційними компонентами необхідно звужувати компоненти, які являють собою результат такого синтезу. Тому на рис. 1 зображена схема синтезу, яка відображає одну зі звужених компонент синтезу двох об'єктів, один з яких пов'язаний з ризиком, а другий — з інформаційною компонентою, що відображає об'єкт дослідження ризику.

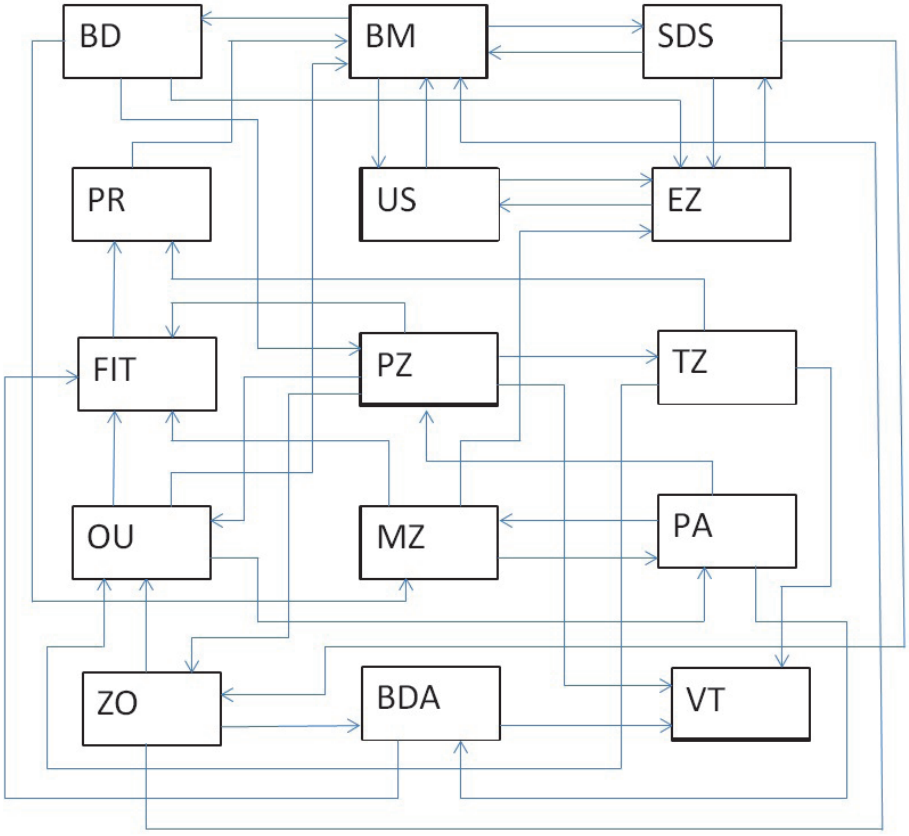

Рис. 1. Функціональна блок-схема результату синтезу ISU та SUB

На рис. 1. використані такі позначення: *BD* — блок діагностики; *BM* — блок моніторингу; *SDS* — система доступу; *PR* — система прогнозування атак; *US* — управління зовнішніми приладами, що безпосередньо пов'язані з поліграфічним обладнанням; *EZ* — модуль елімінації загроз; *FIT* — блок розширення інтерпретаційних описів; *PZ* — блок прикладних задач, що безпосередньо реалізують управ-

ління друкарським обладнанням; *TZ* — визначення поточного значення ризику системи; *OU* — оперативне управління *ISU*; *MZ* — модифікація засобів захисту; *PA* — протидія атакам; *ZO* — системний зв'язок між *ISU* та *SUB*; *BDA* — база даних; *VI* — відображення поточного стану системи.

Особливістю цієї схеми є наявність безпосередніх зв'язків між модулями систем *ISU* та *SUB* і окремого функціонального блоку зв'язку *ZO*. Це зумовлено тим, що на відміну від системи *ISU*, яка функціонує неперервно, оскільки вона здійснює управління *TPP*, система *SUB* може активізовуватися в певні моменти часу, які визначаються різними факторами, насамперед наявністю атак або інших втручань у систему. Система моніторингу *SUB* безпосередньо проводить моніторинг визначених чутливих елементів системи з ціллю виявлення втручання зі сторони зовнішнього середовища. Результатом такого втручання може виявитися зміна параметрів у прикладних задачах управління. У цьому випадку з боку прикладних задач через систему доступу передаються в систему *SUB* дані про аномалії, які виникли в системі розв'язку прикладних задач. Із системи доступу ця інформація потрапляє у модуль зв'язку між системами, який на рис. 1 позначений символами *ZO*, і відповідна інформація потрапляє в модуль оперативного управління *OU* та в модуль моніторування *BM*. Якщо отримана інформація є критичною для *TPP*, то адміністратор реалізує втручання в процес управління. Якщо ситуація не є критичною, то активізується модуль моніторингу, який повинен виявити причини відповідних відхилень. Коли система *SUB* функціонує одночасно або паралельно з системою *ISU*, то в цьому випадку системою використовуються модулі з *SUB* безпосередньо через зв'язки з відповідними модулями *ISU*, які реалізуються відповідно до логіки роботи *SUB* та подій, що в процесі роботи *SUB* виникають у межах системи *SUB*. Це дає змогу реагувати на негативні фактори безпосередньо після їх виявлення в результаті їхньої дії на систему *ISU*.

Наступними фрагментами функціонування синтезованої системи є виявлення траєкторії функціонування, яку реалізує атака A_i, що дає можливість:

- виявити загрозу, наявну в рамках системи ISU, завдяки використанню якої атаці вдається сформувати інтруз $Jt(a_i)$, що безпосередньо є засобом реалізації атаки;
- локалізувати інтруз;
- виявити початкову інформацію про ціль функціонування відповідного інтруза;
- виявити міру здійсненого негативного впливу на *ISU*, який відповідний інтруз встиг реалізувати в середовищі *ISU* чи в окремих його фрагментах.

Можливостями функціонування синтезованої системи є:

- можливість отримання інформації про тип можливої атаки;
- інформація про тип інтруза, який може бути сформований відповідною атакою;
- інформація про метод, за допомогою якого можуть бути реалізовані наведені вище фактори;

Відомо, що ціллю більшості атак є формування певної програмної компоненти, яка б у відповідному програмному середовищі могла реалізовувати процес досягнення цілі, що стоїть перед атакою, та є сформована відповідною небезпекою Nd_i.

Здебільшого атаки класифікуються за характерними для них ознаками:

– за типом загрози, наявної в *ISU*, що використовується атакою для переходу у вигляд $Jt(a_i)$ в середовищі атакованого об'єкта, в розглянутому випадку — у середовищі *ISU*;
– за характеристикою цілі, для досягнення якої відповідна атака активізується і передається до об'єкта атаки.

Перш ніж детальніше розглядати процеси синтезу, приймемо такі положення.

Положення 1. Оскільки система *ISU* являє собою систему управління, в якій не передбачається проводити дослідження стосовно тих або інших реалізацій алгоритму, то всі алгоритми, що реалізуються в *ISU*, переважно являють собою явні аналітичні або логічні функції чи їх синтез.

Положення 2. Оскільки система *ISU* пройшла етап дослідної експлуатації, то відомі множини значень усіх аргументів і функцій, використаних в *ISU*, а також відомі всі області визначень для бінарних змінних, що використовуються в логічних алгоритмах.

Положення 3. Технологічні процеси, якими передбачається керувати, є відомими і не потребують попередніх апробацій роботи алгоритмів чи процесів управління ними.

Положення 1 дає змогу прийняти та використовувати уявлення про τ-функції для реалізації процесів управління. Це означає, що, враховуючи вихідні дані, можна проходити по ланцюгу реалізації окремої функціональної залежності, починаючи від аргументу та закінчуючи значенням функції, що подається у вигляді формального запису таким чином:

$$\omega_i(d_1, \ldots, d_n)=\{TB_m [x_m (a_m, b_m)\rightarrow\ldots\rightarrow TB_n [x_n (a_n, b_n)]\},$$

де $\{d_1, \ldots, d_n\}$ — вхідні дані, які для зручності об'єднуємо однією змінною x_m. Переважно в системах управління технічним обладнанням, процес функціонування якого важко піддається формальному опису, використовують підхід, описаний нижче.

Формують логіку функціонування відповідного екземпляра обладнання в межах одного циклу. Для такої логічної функції встановлюють логічні змінні та задають для них бінарні області інтерпретації.

У рамках такого загального, формального опису процесу вибирають вузли, частина процесу яких, що відповідає вузлу, може описуватися аналітичною функцією чи експериментально встановленою апріорною функцією. Для всіх цих функцій відомі множини допустимих значень вхідних та проміжних даних, що встановлені на етапах дослідної експлуатації та дослідної реалізації відповідного технологічного процесу [4]. Отже, процес управління на рівні реалізації аналітичних функцій може будуватися на основі використання τ-функцій, які оперують таблицями відомих множин значень вхідних параметрів, відомих множин проміжних значень параметрів функцій та відомих множин значень аргументів. У цьому випадку процес управління (якщо відомі значення вхідних параметрів) полягає у переході до проміжних значень цих параметрів, що вибираються з чергових таблиць TB_i на основі використання τ-функцій. Таким способом послідовно реалізований обчис-

лювальний процес доходить до відповідних значень самої функції. Цей процес зручно відобразити у вигляді таких секвенцій:

$$x_i\,(a_i,\, b_i) \rightarrow \tau_1\,[x_{(i\text{-}1)}\,(a_{(i\text{-}1)},\, b_{(i\text{-}1)})] \rightarrow \tau_2\,[x_{(i\text{-}2)}\,(a_{(i\text{-}2)},\, b_{(i\text{-}2)})] \rightarrow \ldots \rightarrow \tau_i\,[y_i\,(a_i,\, b_i)].$$

Як було зазначено, функція τ, по суті, апроксимує процес обчислення між двома послідовними змінами аргументу $x_{i\text{-}k}(a_{i\text{-}k},\, b_{i\text{-}k}) \rightarrow x_{i\text{-}(k+1)}(a_{i\text{-}(k+1},\, b_{i\text{-}(k+1)})$, де a_i, b_i представляють координати клітини таблиці, в якій розміщені необхідні проміжні значення аргументу, серед усіх можливих його значень, що знаходяться у відповідній таблиці $TB_{i\text{-}(k+1)}$. У цьому випадку τ-функція визначає за попередніми координатами $a_{i\text{-}k}$, $b_{i\text{-}k}$ таблиці $TB_{i\text{-}k}$, які визначають клітину в таблиці, де містяться значення $x_{i\text{-}k}$, нові значення координат, де знаходяться наступні проміжні значення параметра x_i, що розміщуються в таблиці $TB_{i\text{-}(k+1)}$. Отже, синтез двох компонент, одним з яких є обчислювальний процес з послідовністю обчислювальних даних $x_i \rightarrow y_i$, з процедурою переходу від елемента множини даних $x_{i\text{-}k}$ до відповідного елемента множини даних $x_{i\text{-}(k+1)}$. У розглянутому випадку принциповими є такі фактори:

– створення системи τ-функцій для реалізації процесу переходу від одних даних до наступних до того часу, поки процес не дійде до даних функції y_i;
– створення таблиць даних TB_i, які в рамках вибраної структури містять усі значення проміжної величини аргументу x_i.

Завдяки такому синтезу можливо простежувати кожний ланцюг ω_i загальної послідовності ланцюгів, яку проходив інтруз $Jt(a_i)$, перш ніж його змінні прийняли відповідні значення. Якщо цей інтруз являє собою фрагмент обчислювальної або аналітичної функції, то існує можливість простежити це місце у відповідному ланцюгу. Така заміна може відбутися тільки в тому випадку, якщо існує загроза, що проявляється в здатності підміняти τ-функції. Цю ситуацію можна проілюструвати, використовуючи звичайні аналітичні функції. Нехай маємо деяку функцію, що в аналітичній формі задається у вигляді $y = ln\, x \cdot sin\, x$. У цьому випадку прикладом формування інтруза $Jt(a_i)$ може бути заміна фрагмента sin$x$ на cos$x$, що призведе до зміни функції, в якій зацікавлена атака. Зацікавленість атаки Ai має умовний характер, оскільки атаку формує небезпека Nb_i, яка відображає свідомі наміри несанкціонованих учасників відповідних процесів організації певного технологічного процесу.

Крім аналітичних і обчислювальних алгоритмів, у системі *ISU* використовуються логічні алгоритми щонайменше на загальному рівні управління технологічними установками. Враховуючи складність управління такими об'єктами, можна стверджувати, що логічні алгоритми також використовуються на рівні розв'язання окремих задач управління. Прикладом можуть бути задачі, пов'язані з необхідністю аналізу різних перемикачів, дискретних регуляторів, перехід деяких значень через встановлені пороги та інші. Тому потрібно розглянути можливі методи простежування траєкторії логічних перетворень, що відбуваються відповідно до прийнятих логічних формул. Припустимо, що всі змінні логічних формул мають інтерпретацію бінарних величин з власними областями визначення, а також, що в рамках реалізації процесів управління застосовуються оператори вузького числення [5]. Опе-

раторами, які використовуються в цьому випадку, є {&, ∨, →, ¬}. Приймемо, що логічна формула у вигляді її програмної реалізації сформована таким чином, що в ній передбачені пріоритети виконання логічних операцій, прийнятих у математичній логіці, та взяті до уваги дужки, що використовуються в логічних формулах та додатково визначають пріоритети виконання тих чи інших логічних операцій. Це приводить до того, що стандартний запис логічної формули, прикладом якої може бути:

$$(x_1 \& x_2) \rightarrow (x_3 \vee (x_4 \rightarrow x_5) \& x_6,$$

де x_1, x_2, x_3, x_4, x_5, x_6 — довільні логічні змінні. Після програмної реалізації ця формула може бути представлена у вигляді:

$$[(x_1 \& x_2) \Rightarrow a_1] * \{[(x_4 \rightarrow x_5) \vee x_3 \& x_6] \Rightarrow a_2\} * [(a_1 \rightarrow a_2)],$$

де a_1, a_2 — результати відповідних перетворень, що зберігаються тимчасово в пам'яті, «⇒» — знак, що означає пересилку результатів у пам'ять під адресами a_1, a_2 відповідно, * — конкатенація незалежних фрагментів логічної формули, яка відповідає порядку реалізації цих фрагментів у відповідній програмі. Тоді можна записати деяку логічну формулу $L(x_1, x_2, x_3, x_4, x_5, x_6)$ у вигляді відповідного ланцюга, логічних перетворень та конкатенацій відповідних незалежних фрагментів формул. У рамках наведеного вище прикладу такий ланцюг можна записати у вигляді:

$$\omega_L = [(x_1 \& x_2) \Rightarrow a_1] * [(x_4 \rightarrow x_5) \vee x_3 \& x_6] \Rightarrow a_2] * [a_1 \rightarrow a_2].$$

Відзначимо, що операції, які мають однакові пріоритети, виконуються у порядку їх використання у відповідній формулі, наприклад операції * і ∨.

Локалізація місця виникнення в логічному ланцюгу аномальної ситуації, на відміну від ланцюга, що відображає процес обчислень, не проводиться послідовно у порядку, визначеному послідовністю обчислень логічних функцій. Це зумовлено тим, що виявлення аномалії може ґрунтуватися на використанні логічних перетворень, які не мусять приводити до елімінації змінних, що зумовлюють виникнення таких аномалій. У випадку виникнення таких аномалій на логічному рівні, які можуть свідчити про виникнення $Jt(a_i)$, необхідно визначитися з критеріями, які можуть відповідати відповідним аномаліям. До таких критеріїв належать:

- виникнення суперечності при перетворенні деякої формули L_i з одної форми представлення в іншу форму, еквівалентну до початкової форми представлення логічного виразу;
- зміна логічного значення формули за умови, що всі початкові значення змінних передбачають існування певного наперед заданого значення;
- зниження міри чутливості логічної формули до зміни значень логічних змінних, що входять у відповідну формулу.

Виникнення суперечності являє собою найбільш загальний випадок виникнення аномалій в L_i, який відбувається на рівні загальності, що відповідає теорії математичної логіки, що інтерпретується на абстрактній предметній області типу теорії множин, формальної арифметики та ін. Алгоритми визначення такого типу аномалій досить широко досліджені в математичній логіці і прикладом такого алгоритму може бути алгоритм Патнема. Виникнення такого типу аномалії досить легко виявити через її загальність, бо наявність суперечності дає змогу визначити

значення відповідної формули, оскільки вона може набувати значення 0 і 1 при еквівалентних перетвореннях.

Висновки. Зміна логічного значення формули L_i під час її обчислення є менш помітною, якщо ця зміна зумовлена виникненням аномалії в L_i. Річ у тому, що будь-яке значення логічної формули L_i є допустиме і означає тільки те, що в предметній області відбулися зміни, що призвели до відповідних змін в L_i. У цьому випадку для виявлення аномалії необхідно аналіз L_i розширити аналізом інтерпретації поточного стану предметної області W_i з ціллю виявлення, чи в W_i наявні зміни, які можуть спричинити зміну значення L_i. Практично це означає, що у процесі аналізу відповідної L_i аналізують інтерпретацію значення кожної змінної в W_i. При цьому порівнюють, чи інтерпретація поточних значень x_i або $l_{ij} \in L_i$ відповідає інтерпретації поточного стану W_i. Якщо така відповідність є, то в L_i аномалії немає. Якщо відповідність інтерпретації x_i чи $l_{ij} \in L_i$ порушується, то в аналізовану фрагменті виникла аномалія.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малихин В. И. Финансовая математика: уч. пособие для вузов / В. И. Малахин. — М. : ЮНИТИ-ДАНА, 2000.
2. Мак-Клар С. Секреты хакеров. Безопасность сетей — готовые решения / С. Мак-Клар, Дж. Скембрей, Дж. Курц. — М. : Издательский дом «Вильсон», 2002.
3. Баранов А. В. Системная интеграция и безопасность компьютерных сетей / А. В. Баранов, С. А. Петренко // Конфидент / А. В. Баранов, С. А. Петренко. — № 2. — 2001. — С. 34–38.
4. Черноруцкий И. Г. Оптимальный параметрический синтез: електротехнические устройства и системы / И. Г Черноруцкий. — Л. : Энергоатомиздат, 1987.
5. Карри Х. Б. Основания математической логики / Х. Б. Карри. — М. : Мир, 1960.

REFERENCES

1. Malihin, V. I. (2000). Finansovaja matematika: uch. posobie dlja vuzov. Moscow: JuNITI-DANA (in Russian).
2. Mak-Klar, S., Skembrej, Dzh., & Kurc, Dzh. (2002). Sekrety hakerov. Bezopasnost' setej – gotovye reshenija. Moscow: Izdatel'skij dom «Vil'son» (in Russian).
3. Baranov, A. V., & Petrenko, S. A. (2001). Sistemnaja integracija i bezopasnost' komp'juternyh setej. Konfident, 2, 34–38 (in Russian).
4. Chernoruckij, I. G. (1987). Optimal'nyj parametricheskij sintez: elektrotehnicheskie ustrojstva i sistemy. Lviv: Jenergoatomizdat (in Russian).
5. Karri, H. B. (1960). Osnovanija matematicheskoj logiki. Moscow: Mir (in Russian).

SYNTHESIS OF RISK MODELS WITH INFORMATION COMPONENTS

B. V. Durnyak, T. M. Maiba

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

The article reviews the processes of synthesis of risk models with information components that directly affect the risk size. It describes the factors that could significantly affect the risk size. It deals with the feasibility of the management process of technological processes based on the performance of τ-functions that operate on tables of the known set of values of input parameters, the known sets of functions intermediate parameters and the known sets of arguments values.

Keywords: *risk model, synthesis process, attacks, threats.*

Стаття надійшла до редакції 11.03.2016.
Received 11.03.2016.