УДК 004.942

СИНТЕЗ МОДЕЛІ РИЗИКУ З СИСТЕМОЮ ЗАХИСТУ ІНФОРМАЦІЙНОГО КОМПЛЕКСУ

Б. В. Дурняк, Т. М. Майба, В. І. Сабат

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

Досліджено моделі ризику та їхній взаємозв'язок із засобами безпеки в системі захисту інформаційного комплексу. Висвітлено основні поняття ризику та безпеки. Впроваджені умови та визначення, на основі яких можна будувати та аналізувати математичні моделі ризику.

Ключові слова: *ризик, безпека, система захисту, засоби захисту.*

Постановка проблеми. Поняття ризику є ключовим у системі безпеки, адже без його визначення і аналізу неможливо побудувати систему захисту, адекватну до наявних загроз. За класичною теорією ризик — це вірогідність втрат, що вимагає захисту. Без ризику не потрібен і захист [1].

Більшість інформаційних систем доповнюються засобами захисту, які об'єднуються в систему захисту [2]. В межах цих систем, крім функцій безпосереднього захисту, реалізуються функції діалогу з користувачем, завдяки яким він отримує інформацію про стан захисту системи, що може являти собою також деяку міру захищеності, яку на поточний момент має система. Отже, поширеною інтерпретацією поняття ризику є інтерпретація величини ризику як деякої небезпеки, що може бути реалізована і, як наслідок, призведе до втрат. Це означає, що ризик здебільшого виявляє деяку оцінку можливих втрат.

Аналіз останніх досліджень та публікацій. Ризик та безпека є тісно пов'язані між собою поняття в системі захисту, тому на цю тематику існує досить багато досліджень і публікацій. Зокрема, поняттям ризику присвячені праці таких вітчизняних та зарубіжних учених: Б. Андрушківа, В. Базилевича, Дж. Банністера, З. Васильченко, В. Вітлінського, В. Галасюка, В. Гранатурової, А. Джонса, А. Камінського, В. Кравченка, Є. Кузьміна, І. Мойсеєнко, Ф. Найта, В. Осецького, А. Пересади, Р. Пікус, А. Старостіни, В. Федоренка, Р. Чаретта, А. Чухна, С. Ткач та інших. Визначаючи ризик в інформаційних системах поліграфічних підприємств, можна керуватись класичними прийомами, що базуються на аналізі та визначенні можливих загроз і вразливостей в їхній системі безпеки. Втім, серед наявних літературних джерел досить мало інформації про створення моделей ризику, які б автоматизували цей процес визначення ризику в системі захисту інформаційного комплексу поліграфічних підприємств.

Виклад основного матеріалу дослідження. На відміну від ризику, рівень безпеки вказує, наскільки небезпечна з погляду можливих втрат ситуація, наявна у

відповідній інформаційній системі чи в системі управління. Розгляньмо деякі відмінності між ризиком і безпекою, які обґрунтовують доцільність, крім рівня безпеки, користуватися величиною ризику.

Першою відмінністю параметра ризику від параметра безпеки є наявність деякого прогнозування, яке характеризує поняття ризику. Ризик передбачає оцінку деякого майбутнього, на відміну від констатації факту, що забезпечує уявлення про рівень безпеки.

Другою особливістю ризику є оцінка деякої події, яка має або може відбутися у майбутньому, а ризик у цьому випадку означає, до чого може призвести відповідна подія, зважаючи на її негативний ефект, причому ризик у цьому разі безпосередньо пов'язується з відповідною подією.

Ризик щодо інтерпретації є величиною, яка використовується для оцінки втрат, зумовлених негативною дією деякої події. У зв'язку з цим ризик зазвичай оцінюється величиною відносною, наприклад у відсотках або у вигляді величини втрат, до яких може призвести певна подія.

З огляду на вказані особливості зазначимо, що величина ризику не може бути величиною точною, а її визначення має ґрунтуватися на використанні приблизних за своєю природою методів та ймовірних даних. Ризик прийнято інтерпретувати як оцінку, що стосується негативних характеристик певної дійсності. Загалом, можна вважати, що ризик застосовують для оцінки подій, які можуть статися, та мають негативну інтерпретацію. Тому ціллю використання ризику є визначення необхідних дій, які призводять до його зменшення або до елімінації ризику загалом. Ризик ніколи не використовується, якщо нема потреби застосовувати оцінки негативного характеру про деякі події, які мають відбутися у майбутньому.

Враховуючи наведені вище особливості інтерпретації поняття ризику, можна стверджувати, що синтез моделей ризику з системою захисту інформації полягає в оцінці можливості зниження рівня безпеки системи, за умови, що таке зниження є негативним. Необхідність врахування цієї умови визначається тим, що уявлення про ризик пов'язане з негативними явищами, які передбачається оцінювати. Потреба використання зазначеної умови ґрунтується на тому, що величина рівня безпеки Be_i може не тільки збільшуватися, а й зменшуватися. У другому випадку зміни величини Be_i інтерпретація цієї зміни може мати позитивний характер. Це пов'язано з тим, що гарантування певного рівня безпеки Be_i потребує деяких затрат, а гарантування безпеки, яке називатимемо захистом, потрібне лише в тому випадку, коли виникають зовнішні атаки на інформаційну керівну систему *ISU,* що зменшують рівень безпеки. Якщо таких атак на *ISU* нема, то недоцільно зазнавати затрат для підтримування рівня безпеки $Be_i = \alpha$, а можна цей рівень знизити до конкретної межі: $Be_i = \beta$, де $\beta < \alpha$. У цьому випадку зниження рівня Be_i не може інтерпретуватися зміною величини ризику *R(t)* процесу функціонування системи *IUS.*

Для коректної реалізації процесу синтезу *R(t)* і Be_i системи *ISU* приймемо такі умови.

Умова 1. Величина ризику *R(t)* повинна обчислюватися на основі статистичних даних або ймовірних параметрів, які характеризують фактори, стосовно яких обчислюється величина ризику.

Умова 2. Обчислення величини ризику мають ґрунтуватися на використанні методів прогнозування.

Умова 3. Величина ризику повинна стосуватися подій або змін умов функціонування об'єкта, які можуть відбутися через вибраний період часу ΔT.

Умова 4. На відміну від задач прогнозування, величина ризику повинна бути тісно пов'язана зі зміною параметра, дією фактора чи іншими подіями, які безпосередньо зумовлюють зміну величини ризику *R(z)*. Для того щоб розділити міру безпеки системи з оцінкою ризику, приймемо такі умови.

Умова 5. Міра безпеки системи Be_i відображає наявний у системі рівень безпеки на поточний момент часу.

Умова 6. Міра безпеки Be_i вимірюється на основі даних, які відображають порушення безпеки системи.

У межах прийнятих умов уважатимемо, що рівень безпеки Be_i вимірюється співвідношенням кількості успішних атак до кількості всіх атак, які реалізувалися стосовно *ISU*. Кількість успішних атак визначається на основі аналізу та виявлення аномалій, які виникають внаслідок дії таких атак, та на основі проведення аудиту системи, стосовно якої визначається Be_i. Отже, величину Be_i можна визначати за таким співвідношенням:

$$Be_i = \sum_{i=k}^{k} \left(\alpha_i ua_i\right) \Big/ \sum_{j=1}^{n} \beta_j a_j,$$

де α — коефіцієнт ефективності успішної атаки ua_i; k — кількість успішних атак; β_j — ефективність атаки a_j, що закладається залежно від типу атак та типу об'єкта атаки; a_j — окрема атака. Кількість знешкоджених або анульованих атак, які здебільшого реєструються, описується співвідношенням:

$$va_i = \left(\sum_{j=1}^{n} \beta_j a_j \right) - \left(\sum_{i=1}^{k} \alpha_i ua_i \right).$$

Кожний тип безпеки B_v, B_u, B_g і B_j зумовлений відповідними атаками. Наприклад, B_v визначається відмовою апаратних компонент. З одного боку, відмова апаратної компоненти може інтерпретуватися як атака. В цьому випадку відповідна атака являє собою подію, яка не зумовлена дією зовнішніх факторів. Вказаний тип атаки може активізуватися зовнішніми факторами, але цієї можливості розглядати не будемо, щоб забезпечити повну однозначність серед множини атак. Очевидно, така відмова може статися і для програмних компонент. Якщо в першому випадку виникнення відмови може бути зумовлене фізичними процесами, що відбуваються у програмних компонентах, то в другому випадку відмова може статися через те, що в програмі трапилась помилка, яку не зауважили на етапі тестування готового програмного продукту. В першому випадку виникнення атаки описують параметри надійності апаратних елементів, а в другому — параметри, які характеризують

ймовірність того, що після тестування у програмі залишилась певна кількість помилок. Прикладом моделі, яка описує наявність помилок, що залишилися в системі програм після тестування, може бути таке співвідношення:

$$f_0 = \ln\left(\begin{smallmatrix} N \\ u \end{smallmatrix}\right) + \sum_{j=1}^{l} N_j \ln N_j + \sum_{j=1}^{l} \left(N - N_j\right) \ln\left(N - N_j\right) - N \ln N,$$

де N — загальна кількість помилок у програмі; U — сума помилок, виявлена t -незалежними тестами, причому приймається, що $U < N$; N_i — кількість помилок, які виявлені i-им тестом [3]. Очевидно, що в першому і другому випадку події, які полягають у виникненні відмов, мають імовірнісний характер. Зазначимо, якщо ймовірнісні оцінки цих подій не змінюються, то їхня поява відповідає певному рівню безпеки Be_i. Оцінка ризику виникає тоді, коли виникає передумова зміни відповідної ймовірнісної оцінки випадкових процесів, які призводять до зміни величини безпеки системи Be_i. Такими передумовами можуть бути не тільки виникнення зовнішніх факторів, а й зміни, які виникають у рамках функціонування системи *ISU*. Прикладом таких змін може бути зміна режиму роботи *ISU,* пов'язана з потребою зміни структур *TPP*. Це може бути зумовлено необхідністю випуску нової продукції та іншими факторами, пов'язаними з *TPP*. Наведений приклад ілюструє один із випадків, коли, крім величини Be_i деякої системи, потрібно обчислювати величину ризику *R(t)*.

Одна з методик визначення оцінки ризику *R(t)* може використовуватися у такому випадку. Приймемо, що в рамках *TPP* застосовується *ISU,* на яку можуть впливати зовнішні та внутрішні фактори. Для забезпечення певної функціональної стабільності система управління *ISU* має гарантувати заданий рівень безпеки функціонування Be_i. Інші компоненти системи *TPP* не розглядатимемо. Якщо зовнішні чи внутрішні стимулювальні фактори виникають випадково, але оцінки цих імовірних подій є сталі, то засоби захисту *ISU* на основі відомих оцінок імовірності виникнення стимулювальних факторів можуть активізувати засоби моніторингу та протидії негативному впливу на *ISU* відповідних факторів. Якщо виникають відомі передумови зміни таких оцінок, то потрібно обчислювати величину ризику зниження рівня безпеки Be_i, де $Be_j \prec Be_i$, або величину ризику, описану співвідношенням: $R(t) \le Be_i - Be_j$, що означає зниження рівня безпеки. Для того щоб обчислити величину *R(t)*, було б доцільно володіти даними про відповідні передумови, які позначатимемо літерою $H\left(h_i\right)$, де h_i — певні параметри передумови *H*. Якщо б така передумова *H* була повністю відома, то б не було потреби обчислювати ризик *R(t)*, а відразу можна б було обчислити нові ймовірнісні параметри факторів, які впливають на рівень безпеки. На основі таких оцінок можна було б модифікувати дисципліну моніторингу відповідних атак та активізувати відповідні засоби захисту, які визначають складові загальної безпеки B_v, B_u, B_g. Тоді доцільно визначити параметр, за допомогою якого можна оцінити загальну характеристику для всіх складових. У теорії ймовірності для цих цілей використовують поняття про оцінку параметрів [4]. Такі оцінки описують такі характеристики: незміщеність оцінки; ефективність оцінки та обґрунтованість оцінки. Незміщеність оцінки оз-

начає, що оцінка $\tilde{\theta}$ параметра θ відповідає співвідношенню $\mu\left(\tilde{\theta}\right)=\theta$, де μ — математичне очікування. Якщо незміщена оцінка має найменшу дисперсію серед усіх оцінок параметра θ, то така оцінка є ефективною, і якщо для оцінки $\tilde{\theta}$ виконується нерівність, яка відповідає закону великих чисел, або наявне таке співвідношення: $\lim_{n=\infty}\left\{P\left|\tilde{\theta}-\theta\right|<\varepsilon\right\}=1$, тоді оцінка $\tilde{\theta}$ називається обгрунтованою. Однією з найпоширеніших оцінок, які використовують для оцінювання параметрів, є випадкова величина, що дорівнює сумі квадратів *n*-незалежних випадкових величин u_i, кожна з яких підпорядковується нормальному закону розподілу з параметрами $\mu = 0$ і $\sigma^2=1$, називається випадковою величиною з розподілом χ^2, та описується співвідношенням:

$$\chi^2=\sum_{i=1}^{n}u_i^2,$$

де $u_i^2=\left(\omega/\sigma_i\right)^2$, $\omega^2=\left(\chi_i-\mu\right)^2$, μ, σ — математичне очікування і дисперсія, χ_i — ряд незалежних спостережень, кожне з яких підпорядковується нормальному законові розподілу. Диференційну функцію розподілу χ^2 з *k*-степенями вільності запишемо так:

$$f\left(\chi^2\right)=L(n).\chi^{n-2}.e^{-\chi^2}/2,$$

де $L(n)$ — коефіцієнт, який залежить від величини вибірки; χ — поточна змінна; *n* — кількість елементів у вибірці. В задачі, яка розглядається у нашому випадку, цей параметр потрібно визначити для того, щоб можна було оцінити можливість спільного використання причин, які зумовлюють можливість небажаного зниження рівня безпеки і, як наслідок, збільшують величини ризику, який характеризує можливість невиконання замовлень на виробництво продукції. Якщо параметр χ^2 виявиться більшим від прийнятої границі, то це означає, що використовувати всі фактори, які спричиняють підвищення ризику спільно недопустимо, оскільки кожна з причин матиме розподіл випадкових значень, які можуть домінувати над іншими розподілами. В цьому випадку потрібно обчислити ризики виникнення недопустимих ситуацій окремо для кожної з причин, що призводять до відхилень поточних значень рівнів безпеки, до яких належать B_g, B_v, B_u і B_i, які в цьому випадку зумовлюватимуть відповідні складові величини ризику R_g, R_v, R_u і R_i. Тоді загальний ризик R_z визначатиметься як функція наведених складових:

$$R_z=f\left(R_g,R_v,R_u,R_i\right).$$

Однією з особливостей оцінки ризику *R(t)* є оцінка змін, які можуть відображатися в системі в разі активізації деякої події за допомогою зовнішніх факторів. На рівні якісної інтерпретації це означає, що потрібно оцінити ризик погіршення ситуації в системі під час реалізації тієї чи іншої дії на систему. Оскільки на систему незалежно від події, стосовно якої розглядається ризик, діють зовнішні фактори, які призводять до зниження рівня безпеки Be_i, у випадку використання ризику відбувається подія і, відповідно, зовнішній фактор, який відрізняється від відомих негативних факторів, проти яких використовується система безпеки *Be*. Для того щоб відрізняти ці події між собою, введемо такі визначення.

Визначення 1. Події, що негативно впливають на деякий об'єкт, захист від яких реалізується засобами захисту, що управляються системою безпеки *Be* і здебільшого є відомими системі безпеки, називатимемо регулярними негативними факторами *RNF*.

Визначення 2. Події, що можуть негативно впливати на об'єкт захисту, які є одноразовими стосовно дії на відповідну систему, називатимемо одинарними негативними факторами (*ONF*).

Якщо одинарні негативні фактори повторюватимуться з частотами, близькими до повторень *RNF*, то *ONF* переходить у категорію *RNF* і їхня дія оцінюється системою *Be*, а не засобами обчислення ризику *R(t)*. Перехід окремих факторів з *RNF* в *ONF* не розглядається, бо до моменту такого переходу система *Be* має достатньо інформації про функціонування факторів класу *RNF*, і тому немає сенсу говорити про ризик впливу такого фактора на систему. В цьому випадку фактор типу *ONF* користувач може формувати так, щоб відповідний фактор позитивно діяв на систему. Перш ніж активізувати цей фактор, його досліджують у рамках моделі системи, завдяки чому можна досить точно визначити характер його впливу на *ISU*, тому нема потреби визначати величину *R(t)*. Якщо деякий фактор типу *ONF* формується для дії на *ISU*, але спосіб такої дії може в процесі її активізації змінюватися і вона може переходити в категорію негативних факторів *NF*, то в таких випадках актуальним є визначення ризику того, що відповідний фактор у результаті його дії на *ISU* спричинить негативні зміни, які будуть інтерпретуватися як зниження рівня безпеки. Якщо деякий фактор y_i є залежний від однієї або невеликої кількості змінних $x_{1,\dots,}x_k$, тоді визначити характер дії на *ISU* можна досить точно. Нема потреби визначати величину ризику *R(t)*, яка, за визначенням, має негативну інтерпретацію. Тому величину ризику будемо встановлювати лише для факторів y_i, які є залежними від значної кількості аргументів або незалежних змінних. Нехай базовою моделлю для визначення величини ризику R_i буде множинна регресія, тоді приймемо таку інтерпретацію елементів множинної регресії, яка виражена співвідношенням:

$$\pi(x) = a_0 + a_1 x_1 + \dots + a_n x_n,$$

де a_i — коефіцієнти регресії, які потрібно визначити. Зазвичай такі коефіцієнти визначаються за принципом найменших квадратів, що описується співвідношенням:

$$\left\{ Q = \sum \left[y - \left(a_0 + a_1 x_1 + \dots + a_n x_n \right) \right]^2 \right\} \to Q \min.$$

Послідовно диференціюємо це рівняння по всіх *n* коефіцієнтах та отримуємо систему рівнянь:

$$\begin{gathered} n a_0 + a_1 \sum x_i + a_2 \sum x_2 + \dots + a_n \sum x_n = \sum y \\ a_0 \sum x_1 + a_1 x_1^2 + a_2 \sum x_1 x_2 + \dots + a_n \sum x_1 x_n = \sum x_1 y. \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_0 \sum x_n + a_1 \sum x_1 x_n + a_2 \sum x_2 x_n + \dots + a_n \sum x_n^2 = \sum x_n y. \end{gathered}$$

Наведена система рівнянь перетворюється таким чином, щоб обчислення коефіцієнтів регресії було максимально спрощеним.

Для практичного використання цього підходу потрібно розглянути інтерпретацію всіх елементів моделі, яка б відповідала прийнятним уявленням про ризик та ціль використання обчисленої величини *R(t)*. У рамках системи *ISU* використовують засоби *Zz*, що організовані в рамках системи безпеки $Be_i = \{Zz_1, ..., Zz_n\}$, та засоби визначення ризику функціонування системи R_i. Система *Be* характеризується рівнем безпеки $\mu(Be)$, який залежить від загальної кількості атак та атак, які були елімінованні засобами безпеки *Be*. Що більше атак було знешкоджено, то вищий рівень $\mu(Be)$. Якщо кількість атак, що ініціюються стосовно *ISU*, зменшується, то і кількість атак, які засоби захисту елімінували, також зменшиться. Таким чином, $\mu(Be)$ залишається однаковим, незалежно від того, яка кількість атак активізується стосовно *ISU*. Ризик за своєю інтерпретацією є зворотною величиною до величини безпеки. Інтерпретація безпеки полягає у тому, що величина безпеки характеризує поточний стан можливостей *ISU* з погляду придатності системи до розв'язання основних прикладних задач. Це означає, що для різних класів задач, які розв'язуються в середовищі *TPP*, потрібно забезпечити різні рівні безпеки $\mu(Be) = \alpha$. Тому основною задачею системи безпеки є підтримка певного рівня безпеки функціонування *ISU*, а отже, *TPP*, який дорівнює $\mu(Be) = \alpha_i$. Величина ризику стосовно інтерпретації характеризує можливість виникнення негативних змін в об'єкті і залежно від цього такий ризик вимірюється. Тому для встановлення ризику важливо визначити об'єкт, в якому передбачаються зміни, та з'ясувати, в чому може полягати ризик. Вважатимемо, що ризик полягатиме у зменшенні величини безпеки *Be*. Подальший розвиток інтерпретації цього аспекту не розглядатимемо. Очевидно, що зростання величини безпеки не стосуватиметься ризику. Щоб поняття ризику не дублювало поняття безпеки, припустимо, що ризик визначає величину зменшення рівня безпеки Be_i. Тоді можна ввести таке визначення:

Визначення 3. Ризик являє собою оцінку можливої величини негативної зміни міри безпеки.

Для того щоб можна було говорити про похідну від безпеки, потрібно функцію зміни рівня безпеки представити у певній формі. На якісному рівні це можна зробити так. Нехай у процесі функціонування *ISU* і, відповідно, системи управління безпекою (*SUB*) у кожний фіксований момент часу величина $\mu(Be_i)$ набуває певних значень. Це можна подати у вигляді такого співвідношення: $\mu(Be_i) = \alpha_i$. Тоді рівень безпеки можна визначати за таким співвідношенням:

$$\mu(Be_i) = \alpha_i = \sum_{i=1}^{k} At_i / At_i^n,$$

де At_i — атаки, що виявлені в процесі функціонування *SUB*; At_i^n — усі можливі на момент t_i атаки, які активізувалися щодо *ISU*. Отже, використовуючи вибрану функцію апроксимації, можна отримати наближений опис функції зміни величини $\mu(Be)$:

$$\mu(Be) = f(Be, Be_i, t),$$

де *t* — час функціонування *SUB*. Оскільки *R(t)* — прогнозування оцінки негативної зміни величини безпеки, то подія, з якою пов'язується ризик, може належати до факторів негативного впливу на *ISU*. Такі фактори в цьому дослідженні належать до категорії атак на *ISU*. Тому подія, стосовно якої передбачається визначати величину ризику, знижує рівень безпеки *ISU*, що може відбутися у випадку, якщо виникне подія типу $At_i(ONF)$. З'ясуємо, у чому полягають задачі, які виникають за потреби визначення таким чином сформульованого уявлення про ризик.

Перша задача полягає у прогнозуванні виникнення події $At_i(ONF)$, яка орієнтована на вплив на *ISU* та *SUB*.

Друга задача полягає у визначенні механізму дії $A_i(ONF)$ на *ISU* з метою обчислення величини втрат, до яких може призвести дія цієї події.

Третя задача, яка виникає у зв'язку з оцінкою величини ризику, полягає у синтезі результату прогнозу з величиною втрат, яких завдає активізація $A_i(ONF)$.

Четверта задача полягає у визначенні взаємозв'язків між *ISU*, на яку діє $At_i(ONF)$, та *SUB*, яка має протидіяти відповідному факторові. На основі такого аналізу визначають міру змін, які відбудуться в *ISU* і завдяки захисним функціям *SUB* будуть меншими порівняно зі змінами в *ISU*, які відбулися б у разі невикористання *SUB*.

П'ята задача полягає у необхідності формулювання адекватної інтерпретації величини ризику для *ISU* у результаті можливої дії $A_i(ONF)$. Адекватна інтерпретація полягає у такому:

- визначення величини втрат у результаті отриманої величини ризику;
- вибір одиниць вимірювання таких втрат;
- визначення величини ймовірності виникнення втрат у поєднанні між собою наведених інтерпретаційних описів.

Висновки. Метод розв'язування наведених вище задач реалізується в певній послідовності. Спочатку, застосовуючи регресійні моделі за допомогою статистичних вибірок про можливі атаки, розв'язують задачу прогнозування виникнення $A_i(ONF)$. Завдяки прогнозуванню можна отримати інформацію, коли і за яких умов прогнозована подія виникне [5].

У подальшому розв'язується задача розпізнавання $A_i(ONF)$ на основі моделювання дії можливої атаки на систему. Метою цієї задачі є розпізнавання атаки, що дасть змогу визначити відповідну міру захисту системи *SUB*, внаслідок чого величина негативного впливу $At_i(ONF)$ на *ISU* може бути зменшена.

На наступному етапі розв'язують задачу визначення можливих втрат, які, наприклад, можна проектувати на вартість продуктів, що мають продукуватися *TPP* під управлінням системи *ISU*. Отже, за допомогою описаних методів розв'язку зазначених вище задач стає можливим формування адекватної інтерпретації величини ризику *R(t)*.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Белов Е. Б. Основы информационной безопасности / Е. Б. Белов В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М. : Горячая линия. — Телеком, 2006. — 544 с.

2. Мак-Клар С. Секреты хакеров. Безопасность сетей – готовые решения. 2-е издание / С. Мак-Клар, Дж. Скембрей, Дж. Курц. — М. : Издательский дом Вильямс, 2001. — 656 с.
3. Marciniak J. J. Encyclopedia of Software Engineering 2 Volume Set — 2 Edition / J. J. Marciniak. — Johu Wely & Sons Jnc., 2001. — 1584 p.
4. Печинкин В. А. Теория вероятностей / В. А. Печинкин, О. И. Тескин, Г. М. Цветкова и др.; под ред. В. С. Зарубина, А. П. Крищенко. — М. : Изд-во МГТУ им. Н. Э. Баумана, 1998. — 456 с.
5. Горяинов В. Б. Математическая статистика / В. Б. Горяинов, И. В. Павлов, Г. М. Цветкова и др.; под ред. В. С. Зарубина, А. П. Крищенко. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2001. — 424 с.

SYNTHESIS OF A RISK MODEL WITH SYSTEM OF INFORMATION COMPLEX PROTECTION

B. V. Durnyak, T. M. Maiba, V. I. Sabat

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

The risk models and their relationship with the safety means in the system of information complex protection have been studied. The basic concepts of risk and safety have been reviewed. Terms and definitions on which we can design and analyse mathematical models of risk have been introduced.

Keywords: *risk, safety, protection system, protection means.*

Стаття надійшла до редакції 04.01.2016.