УДК 519.81

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 77-83

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ ПРОГРАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: МОДЕЛІ ЗАГРОЗ І РИЗИКІВ

С.В. Зибін, В.О. Хорошко

Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03680, Україна; e-mail: professor_va@ukr.net

Пропонується підхід до підтримки прийняття рішень для формування комплексних, цільових програм інформаційної безпеки держави при наявності загроз і ризиків, який базується на введенні моделей загроз і ризиків в ієрархію цілей програм (задач) і її цільової оцінки. Модель ризику має фактор ризику, який являється випадковим процесом і має спеціальну ціль. Загроза моделюється спеціальною програмою, яка вводиться в ієрархію цілей.

Ключові слова: підтримка прийняття рішень, моделі загроз і ризиків, інформаційна безпека, ієрархія цілей, цільова оцінка.

Вступ

Комплексна програма забезпечення інформаційної безпеки держави (ПІБД) являє собою сукупність заходів, які об'єднані єдністю глобальної мети й загальними ресурсами [1, 2]. Основні завдання розробки складних ПІБД – відбір програм, що входять в комплексну програму, й розподіл між ними ресурсів. При цьому ПІБД, як правило, може плануватися на великі проміжки часу, тому необхідно оцінювати ефективність програм на заданому інтервалі часу.

При розробці ПІБД слід враховувати можливість виникнення загроз і ризиків, аналізувати їхній вплив і на цій основі передбачати заходи щодо протидії їм або усунення їх. При формуванні ПІБД із урахуванням загроз і ризиків необхідно розв'язувати наступні задачі:

1. Визначення кількісних характеристик впливу загроз і ризиків на ефективність ПІБД;
2. Визначення кількісних показників ефективності програм при наявності загроз і ризиків;
3. Розподіл ресурсів між засобами протидії загрозам і ризикам та програмами, що мають спрямованість на підвищення інформаційної безпеки держави.

Відомі методи розв'язання першої задачі передбачають ідентифікацію ризиків (якісний аналіз), а також оцінювання ймовірностей і розмірів можливого збитку (кількісний аналіз) [3, 4]. Однак при цьому задача оцінки ефективності програм з врахуванням ризиків не вирішується й залишається на розсуд експерта – особи, що приймає рішення (ОПР). Більше того, визначення збитку в абсолютному вимірюванні часто неможливо для складних ПІБД.

Ціль роботи

У роботі пропонуються методи рішення задач ПІБД. Робота складається із двох частин. У першій частині викладається сутність запропонованого підходу й моделі загроз і ризиків, а в другій – методи обчислення кількісних показників відносної ефективності програм ІБД в умовах загроз і ризиків, напрямків виконання ПІБД із урахуванням загроз і ризиків; відносної ефективності заданої множини: загроз і ризиків, засобів протидії загрозам і ризикам.

Основна частина

Метод рішення задачі оцінки відносної ефективності програм при наявності загроз і ризиків природно розробляти на основі методів рішення даної задачі без обліку цих факторів. Найбільше розповсюдження сьогодні одержали мультикритеріальні методи оцінки програм [5]. Галузь їх застосування обмежується двома умовами, яким повинна задовольняти конкретна задача.

Перша умова – наявність множини критеріїв, по кожному з яких можна оцінити окрему альтернативу.

Друга умова – здатність ОПР оцінити тим або іншим способом кожну альтернативу за окремим критерієм.

Перша умова в більшості випадків формування складних ПІБД не виконується через істотну різницю природи програм, що входять у них. Виконання другої умови являється досить проблематичною, коли вибір найбільш оптимального варіанта з декількох або ранжирування такої кількості варіантів вимагає обліку їх оцінок по декільком десяткам взаємозалежних критеріїв. Така ситуація має місце при прийнятті рішень по формуванню складних ПІБД.

Тому методи підтримки прийнять рішень при формуванні ПІБД в умовах загроз і ризиків можна розробляти шляхом модифікації методів цільового оцінювання варіантів [1, 2, 5]. При підтримці рішень по розробці ПІБД відносна ефективність програм повинна оцінюватися як функція часу, задана на інтервалі планування [3]. Тому можливість обліку фактору часу при оцінці програм ІБД принципова для розв'язання задач підтримки рішень такого роду.

Основна ідея запропонованого підходу до аналізу впливу загроз і ризиків при виконанні ПІБД полягає в тому, що події, які спричиняють загрози або ризики, розглядаються як складова частина ПІБД, тобто програми впливу зовнішнього середовища. Тому такі програми-моделі загроз або ризиків включаються в ієрархію цілей ПІБД [6], встановлюються їхні зв'язки з іншими програмами й цілями ПІБД. Таким чином, кожна із програм-моделей загроз або ризиків має хоча б одну ціль або програму, на досягнення якої (ступінь виконання якої) вона безпосередньо впливає. Виходячи із [6], визначимо такі цілі (програми) безпосередніми надцілями програми-моделі загрози або ризику. При цьому вплив загрози й/або ризику, як і інших програм ПІБД, оцінюється ступенем впливу на досягнення головної цілі програми. Ефективність програми ІБД оцінюється за умови наявності загроз і ризиків з врахуванням їх ймовірнісних характеристик. Такий підхід дає можливість розподілити ресурси на відбивання загроз і ризиків нарівні з розподілом ресурсів на програми, що складають сутність ПІБД.

Для реалізації запропонованого підходу необхідно вирішити ряд часткових задач. Перша пов'язана з розробкою математичних моделей загроз і ризиків, що дозволяють включати події, які спричиняють загрозу й/або ризик, в ієрархію цілей ПІБД. Сутність другої задачі полягає в розробці методу кількісного оцінювання впливу загрози й/або ризику. Наступна задача – пошук способу оцінки відносної ефективності програми ІБД при наявності загроз і ризиків.

Аналіз, який визначає загрози дозволяє виявити деякі властивості, що характеризують це поняття. По-перше, слід зазначити, що загроза – це наслідок події, що полягає у виникненні ситуації, яка впливає на виконання ПІБД. Однак загроза являється результатом діяльності певних груп людей на відміну від ризику, який в основному являється наслідком випадкової події. По-друге, інтенсивність впливу загрози на виконання задач ПІБД – це випадкова величина, що змінюється із часом.

Загальним для понять "загроза" і "ризик" є вплив зовнішнього середовища на виконання ПІБД і те, що вони являються наслідком її впливу на виконання ПІБД.

На підставі проведених досліджень сформулюємо визначення.

Визначення 1. Загроза є стан середовища, що впливає на ефективність задач ПІБД, у якому виконується комплексна цільова програма.

Крім того, можна зробити висновок про існування засобів нейтралізації загрози, які впливають на рівень її небезпеки.

Із цього випливає можливість побудови моделі загрози, яка являє собою деяку задачу ПІБД, причому існує хоча б одна задача або ціль, рівень досягнення якої залежить від рівня виконання задачі-моделі загрози (ЗМЗ). Крім того, ЗМЗ може мати в якості підзадач інші задачі, що впливають на її ефективність, тобто заходи нейтралізації загрози.

Таким чином, модель загрози має всі властивості задачі ПІБД із деякими особливостями.

Визначимо у відповідність загрозі r_i деяке число $0 \le M_i \le 1$, яке називається ступенем реалізації загрози, причому $M_i = 0$, при повній відсутності впливу загрози й $M_i = 1$ при максимально можливій її прояві. Крім того, будемо характеризувати загрозу r_i ймовірністю p_t її реалізації в момент часу *t*. Цю величину повинні визначити експерти за допомогою групових методів експертного оцінювання [2, 8].

Визначення 2. Частковий коефіцієнт впливу α_{ij} (ЧКВ) загрози r_i на досягнення її безпосередньої надцілі λ_j (ступінь виконання задачі P_j) є приріст ступеня досягнення надцілі λ_j ступінь виконання задачі P_j), отриманий внаслідок повної реалізації загрози r_i.

У роботі далі, якщо це не викликає різночитань, будемо використовувати термін "надціль" для позначення як цілі, на ступінь досягнення якої безпосередньо впливає задача-модель загрози, так і задачі, на ступінь виконання якої впливає ця загроза.

Для більш адекватного опису задач підтримки рішень щодо комплексного цільового планування з урахуванням загроз і ризиків доцільно враховувати зміни в часі їх впливів. Виходячи із цього будемо говорити про миттєві значення в момент часу *t* коефіцієнта впливу $\alpha_{ink}(t)$ загрози r_i на досягнення її безпосередньої надцілі λ_n, який визначається з виразу

$$\alpha_{ih}(t) = \begin{cases} 0, \ якщо\ t < \tau_{ih}; \\ \beta(\alpha_{ih}, t), інакше, \end{cases} \qquad (1)$$

де α_{ih} – стаціонарне значення коефіцієнта впливу (СЗКВ) загрози r_i на безпосередню надціль λ_h;

τ_{ih} – експертна оцінка затримки впливу загрози r_i на надціль λ_h;

λ – поліноміальна функція, яка описує зміну коефіцієнта впливу в часі.

Так як достовірна інформація щодо точності експертних оцінок коефіцієнтів полінома $\beta(\alpha_{ih}, t)$ відсутня, визначимо в (1) $\beta(\alpha_{ih}, t) = \alpha_{ih}$, тобто будемо враховувати тільки затримку впливу загрози на її безпосередню надціль. Цю величину визначають експерти.

Стаціонарні значення коефіцієнтів впливу $\alpha_{ih} \in A_h, i = (1, n_h),$ безпосередніх підцілей надцілі α_h, серед яких можуть бути загрози, що задовольняють умові $\sum_{i=1}^{nh} |\alpha_{ih}| = 1$.

У загальному випадку загроза r_i є безпосередня підціль декількох надцілей $\lambda_1, \lambda_2, ..., \lambda_h, ..., \lambda_z$, причому будь-яка надціль λ_h має деяку множину $\{\Lambda_h = \Lambda_{hk}\}$ альтернативних підмножин сумісних безпосередніх підцілей, $\Lambda_{hk} \cap \Lambda_{hl} \neq \phi, k \neq l$. Тому можливий випадок, коли $\lambda_i \in \Lambda_{hk}, \lambda_i \in \Lambda_{hl}, k \neq l$,і одна й та сама загроза r_i буде мати різні стаціонарні значення $\alpha_{ihk}, \alpha_{ihl}$ коефіцієнта впливу на одну й ту саму безпосередню надціль λ, які обчислені для різних альтернативних підмножин $\Lambda_{hk}, \Lambda_{hl}$.

Якщо досягнення підцілі λ_i сприяє досягненню її безпосередньої надцілі λ_h, тоді її СЗКВ $\alpha_{ihk} > 0$, інакше $\alpha_{ihk} < 0$. Із вмісту поняття загроз випливає, що часткові коефіцієнти впливу задач, які являються моделями відповідних загроз, від'ємні. Зауважимо, що до початку процесу визначення СЗКВ підцілей ієрархія повинна бути перетворена таким чином, щоб СЗКВ всіх підцілей були доданими. Це досягається заміною підцілей, які негативно впливають на відповідні надцілі, підцілями, які являються їх логічними інверсіями.

Тепер визначимо характеристики загроз. Першою характеристикою, яка визначає тип загрози, є спосіб вираження умов і наслідків її реалізації. Якщо умови реалізації загрози можна виразити результатом виміру деякої однієї, конкретної величини-ресурсу, то така загроза називається кількісною по входу, інакше – якісною.

Оскільки вплив ЗМЗ на досягнення їх безпосередніх надцілей негативний, то для найгіршого випадку ступінь їх виконання при відсутності компенсуючих впливів приймається рівним 1. При цьому ресурс визначається як кількісне вираження умов компенсації загрози, яка приводить до того, що ступінь виконання ЗМЗ буде дорівнювати нулю. Так, ресурс задачі, який являється моделлю загрози "атаки на інформаційні ресурси держави" являє собою суму окремих атак на різні елементи цих ресурсів.

Якщо значення ресурсу кількісної по входу загрози відомо, то така загроза є кількісною по входу визначеною. Значення ресурсу такої загрози однозначно визначається експертами при побудові ієрархії цілей. Якщо ж значення її ресурсу напевно невідомо, то така загроза являється кількісною по входу невизначеною. Для таких загроз визначаються погоджені узагальнені експертні оцінки величини ресурсу [1, 8].

Тому що ЗМЗ завжди являється безпосередньою підціллю якої-небудь цілі або задачі, вона характеризується результатом його виконання. Якщо результат повного виконання загрози можна виразити ефектом, тобто результатом виміру деякої однієї величини, то загроза є кількісною по виходу, а якщо ні, то – якісною по виходу.

Зрозуміло, що при визначенні ступеня досягнення надцілі повинні враховуватися ефекти від досягнення тільки множини її сумісних цілей. Тому що загроза діє незалежно від виконавців ПІБД, слід вважати її сумісної з кожною з підцілей. Тому ЗМЗ входить у кожну підмножину сумісних підцілей тієї надцілі, на досягнення якої безпосередньо впливає загроза. Отже, можна сформулювати наступне визначення.

Визначення 3. Безпосередні підцілі λ_i і λ_j, у тому числі й загрози деякої надцілі λ_S, називаються сумісними, якщо досягнення однієї не виключає можливості або доцільності досягнення іншої, і несумісними в протилежному випадку.

На підставі проведених досліджень приступимо до створення узагальненої моделі загрози. При цьому миттєве значення $M_h(t)$ ступеню реалізації загрози r_h у момент часу *t* визначається в такий спосіб:

$$M_h(t)=\begin{cases}0,\ якщо\ \sup_k \sum_i \alpha_{ihk}(t)\, M_i(t) < \Pi_h;\\ \Pi_h,\ якщо\ \sup_k \sum_i \alpha_{ihk}(t)\, M_i(t) = \Pi_h;\\ f(\sup_k \sum_i \alpha_{ihk}(t)\, M_i(t)),\ якщо\ \Pi_h < \sup_k \sum_i \alpha_{ihk}(t)\, M_i(t) < 1-\sum_q \left|\alpha^{(-)}_{qhk}(t)\right|;\\ 1,\ якщо\ (1-\sum_q \left|\alpha^{(-)}_{qhk}(t)\right|) \le \sup_k \sum_i \alpha_{ihk}(t)\, M_i(t) \le 1;\end{cases} \quad (2)$$

де Π_h – поріг загрози r_h;

$f(\sup_k \sum_i \alpha_{ihk}(t)\, M_i(t))$ – функція ступеня реалізації загрози r_k;

k – номер підмножини Λ_{hk} сумісних безпосередніх підцілей загрози r_k;

i – номер підцілі $\lambda_i \in \Lambda_{hk}$;

$\alpha_{ihk}(t)$ – миттєве значення в момент часу t часткового коефіцієнта впливу підцілі $\lambda_i \in \Lambda_{hk}$ на досягнення загрози r_k, обчислене за умови, що підціль λ_i розглядається як елемент підмножини Λ_{hk} сумісних, безпосередніх підцілей загрози r_k;

$M_i(t)$ – миттєве значення ступеня досягнення підцілі λ_i у момент часу t;

$\alpha^{(-)}_{qhk}(t)$ – миттєве значення в момент часу t часткового коефіцієнта впливу підцілі $\lambda_q \in \Lambda_{hk}$, що негативно впливає на загрозу r_k.

Важливі окремі випадки загроз – це загрози квазілінійна й порогова.

Ступінь M_j виконання квазілінійної ЗМЗ r_j визначається виразом

$$M_j=\begin{cases}\sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh}, якщо \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh}, \le 1;\\ 1, \qquad\qquad якщо \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh}, > 1,\end{cases}$$

де h – номер підмножини Λ_{jk} сумісних, безпосередніх підцілей ЗМЗ загрози r_j;

s – номер підцілі $\lambda_{sjh} \in \Lambda_{jh}$;

α_{sjh} – частковий коефіцієнт впливу підцілі $\lambda_{sjh} \in \Lambda_{jh}$ на досягнення загрози r_j.

Вираз для обчислення M_j ступеня досягнення порогової загрози r_j має наступний вигляд

$$M_j=\begin{cases}1, \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh} \ge \left|1-\sum\limits_{j\in Ji} \alpha_j\right|;\\ 0, в\ іншому\ випадку;\end{cases}$$

де J_i – множина номерів підцілей загрози r_j с негативним впливом.

Тепер приступимо до розробки моделі ризику. Поняття ризику характеризується невизначеністю, пов'язаною з можливістю виникнення в ході реалізації задачі ПІБД несприятливих ситуацій і наслідків [3, 4]. Інакше кажучи, під ризиком слід розуміти наслідок випадкової події, викликаної зовнішніми відносно ПІБД факторами, яка полягає у виникненні ситуації, що впливає на виконання програми ІБД.

Оскільки ризик є наслідок випадкової події, яка чи то відбудеться, чи то ні, тому, залежно від того, чи являється розробник ПІБД оптимістом або песимістом, сутність події, яка викликає ризик, можна сформулювати в одному випадку так, що його виникнення викличе негативний вплив на виконання програми, або так, що воно буде мати позитивний вплив.

Залежно від природи подій, які викликають ризик, розрізняють: техніко-технологічні, політичні, економічні, воєнні, фінансові, екологічні ризики учасників задачі, ризики обставин непереборної сили (форс-мажор) і специфічні ризики [4, 9]. При цьому одна й та сама подія може викликати ризики, які мають зовсім різні наслідки для виконання ПІБД. При цьому ризики необхідно оцінювати, виходячи із системного підходу, з урахуванням мети ПІБД і її структури.

Запровадимо визначення деяких понять.

Визначення 4. Фактором ризику ψ для ПІБД P називається процес ξ_ψ такий, що $\exists p_i \in P\left[V(p_i)\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t)\right]$, де $V(p_i)\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t)$ – відносна ефективність задачі (програми) $p_i \in P$ з урахуванням фактору ризику $\xi_\psi(t)$ і без його урахування, відповідно.

Визначення 5. Індикатором ризику ψ називається фіктивна ціль λ_ψ, єдиної підціллю якої є фактор ризику ψ.

Зазначимо, що фактор ризику є підціль для таких індикаторів ризику як λ_{ψ_1} і λ_{ψ_2}. Підцілі λ_{ψ_1} і λ_{ψ_2} – індикатори ризику, повністю описуються функціями ступеня досягнення цілі. У загальному випадку миттєве значення $M_h(t)$ ступеня досягнення безпосередньої надцілі λ_h у момент часу *t* визначається виразом (2).

При завданні функції досягнення цілі-індикатора ризику необхідно враховувати наступні особливості:

1. Оскільки пороги цілей задовольняють умові [10] $0 \le \prod_h \le 1$, тому значення випадкового процесу $\xi_\psi(t)$, що задає фактор ризику ψ, повинне також задовольняти умові $0 \le \xi_\psi(t) \le 1$;
2. Якщо $\left[\partial M(\lambda_{\psi_1}) / \partial \xi_\psi(t)\right] < 0$, у якості фактору ризику для цілі λ_{ψ_i}, що являється індикатором цього ризику, необхідно вибирати $\left[1 - \xi_\psi(t)\right]$ замість $\xi_\psi(t)$.

Висновки

Пропонується підхід до підтримки прийняття рішень при формуванні комплексних програм забезпечення інформаційної безпеки держави з врахуванням загроз і ризиків. Під загрозою розуміється стан середовища, що впливає на ефективність задач ПІБД, у якому виконується комплексна цільова програма. Ризик визначений як наслідок випадкової події, викликаної впливом зовнішніх відносно ПІБД факторів, що полягає у виникненні ситуації, яка впливає на виконання ПІБД. Запропоновані моделі загроз і ризику.

Список літератури

1. Тоценко, В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / В.Г. Тоценко. – К: Наукова думка, 2002. – 382 с.
2. Орловский, С.А. Проблемы принятия решений при нечёткой исходной информации / В.Г. Орловский – М: Наука, 1981. – 208 с.
3. Згуровский, М.З. Информационный подход к анализу и управлению проектными рисками / М.З. Згуровский, Н.И. Коваленко, К. Кондрак, Э. Кондрак // Проблемы управления и информатики. – 2000. – № 4. – С. 148–156.
4. Грачёва, М.В. Анализ проектных рисков. Учебное пособие для вузов / М.В. Грачёва. – М.: ЗАО «Финстатинформ», 1999. – 216 с.
5. Кини, Р.Л. Принятие решений при многих критериях: предпочтения и замещения / Под ред. И.Ф. Шахнова. – М.: Радио и связь, 1981. – 560 с.

6. Руа, Б. Проблемы и методы принятия решений в задачах со многими целевыми функциями / Б. Руа // Вопросы анализа и процедуры принятия решений // под ред. И.Ф. Шахнова. – М.: Мир, 1976. – С. 20–58.
7. Катренко, А. В. Теорія прийняття рішень: підручник з грифом МОН / А.В. Катренко, В.В. Пасічник, В.П. Пасько. – К.: Видавнича група BHV, 2009. – 448 с.
8. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993. – 278 с.
9. Макаров, И.М. Теория выбора и принятия решений / И.М. Макаров, Т.М. Виноградская, А.А. Рубчинский, В.Б. Соколов. – М: Наука, 1982. – 328 с.
10. Зибін, С.В. Оцінка якості функціонування комплексних систем технічного захисту й систем підтримки ухвалення рішення в їхньому складі / В.О. Хорошко, С.В. Зибін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Вип. 2 (24). – С. 7–15.

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПРИ ФОРМИРОВАНИИ ПРОГРАММ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: МОДЕЛИ УГРОЗ И РИСКОВ.

С.В. Зыбин, В.А. Хорошко

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03680, Украина; e-mail: professor_va@ukr.net

Предлагается подход к поддержке принятия решений для формирования комплексных целевых программ информационной безопасности государства при наличии угроз и рисков, который базируется на введении моделей угроз и рисков в иерархии целей программ (задач) и целевой оценки её. Модель риска имеет фактор риска, который является случайным процессом и имеет специальную цель. Угроза моделируется специальной программой, которая вводится в иерархию целей.
Ключевые слова: поддержка принятия решений, модели угроз и рисков, информационная безопасность, иерархия целей, целевая оценка.

DECISION-MAKING SUPPORT IN THE DEVELOPMENT OF NATIONAL INFORMATION SECURITY PROGRAMS. PART 1: DANGER-AND-RISK MODELS

S.V. Zybin, V.O. Khoroshko

National aviation university
1, Kosmonavta Komarova Avenue, Kyiv, 03680, Ukraine; e-mail:professor_va@ukr.net

The paper presents an approach to decision-making support in the development of comprehensive special-purpose national information security programs in the presence of dangers and risks. The approach relies on the introduction of danger-and-risk models into the hierarchy of program/task targets and on the target-based assessment of the support. The risk model has a random risk factor and a special target. The danger is simulated by a special program which is introduced into the target hierarchy.
Keywords: decision-making support, danger-and-risk models, information security, target-based assessment.