УДК 04.073 **doi:** https://doi.org/10.20998/2522-9052.2021.4.09

О. Г. Лебедєв, В. О. Лебедєв

Харківський національний університет радіоелектроніки, Харків, Україна

Методика аналізу ризиків в інформаційних системах

Анотація. Актуальність. На сьогодні залишається невирішеним завдання управління ризиками в інформаційній системі управління з урахуванням взаємозв'язку різних алгоритмів та моделей для досягнення конкретних результатів щодо управління інформаційно-телекомунікаційними комплексами управління технічними об'єктами. **Мета статті** – розробка методики аналізу та управління ризиками в інформаційних системах управління. Досліджуються шляхи забезпечення ефективності функціонування систем управління в умовах інформаційного протиборства з використанням апарата теорії ігор. Розробляється методика оцінки середнього значення показника якості функціонування системи управління та отримані вирази для оцінки середнього значення показника при різних стратегіях поведінки. Показано, що вирішення проблеми підвищення якості функціонування системи управління, можливе за рахунок застосування змішаної стратегії поведінки системи управління та вибору структури і параметрів системи управління, що збільшують часткові показники якості її функціонування.

Ключові слова: аналіз ризиків; інформаційні системи; системи управління; самовідновлювальна система; загрози інформації; синтез системи.

Вступ

Постановка проблеми. Сучасні системи управління є, як правило, складовою інформаційно телекомунікаційних комплексів управління технічними об’єктами та людьми. Такі комплекси набули розвитку завдяки прогресу в області комп’ютерної техніки, автоматизації управління й технологічних процесів. Прагнення забезпечити високу ефективність таких комплексів управління, мінімізувати фінансові затрати, забезпечити енергетичний та інформаційний захист системи управління, висуває на перший план створення системи аналізу та управління ризиками в інформаційних системах. Методи та алгоритми управління ризиками досить повно описані у міжнародних стандартах та у спеціальній літературі[1-5]. Водночас наразі залишається невирішеним завдання управління ризиками в інформаційній системі управління з урахуванням взаємозв'язку різних алгоритмів та моделей для досягнення конкретних результатів щодо управління інформаційно-телекомунікаційними комплексами управління технічними об'єктами [6-8].

Мета статті – розробка методики аналізу та управління ризиками в інформаційних системах управління.

Виклад основного матеріалу

Для оцінки ймовірності виникнення загрози спочатку наведемо зручну для подальшого розгляду класифікацію загроз інформації. Оскільки кінцевою метою оцінки є (в ідеальному випадку) визначення ймовірності виникнення загрози, виділимо такі джерела загроз: природні – це стихійні лиха, аварії, збої та відмови технічних засобів, інші події, спричинені об'єктивними фізичними явищами, непідконтрольними людині; штучні – погрози, спричинені діяльністю людини. Ці загрози поділяються на ненавмисні (випадкові), спричинені помилками у проектуванні систем та елементів, помилки у програмному забезпеченні, помилки в діях персоналу тощо, та навмисні, пов'язані зі свідомим заподіянням шкоди.

Нехай F функціонал, описуючий якість системи управління в умовах дії загроз[9,10]

$$F\left(G(h,r),I(R),S(L),V(r,t),T(t)\right), \qquad (1)$$

де $G(h,r)$ – функція, яка характеризує енергетичні параметри системи управління; $I(R)$ – функція, яка характеризує стійкість від зовнішніх впливів; $S(L)$ – функція, яка характеризує структурну надійності програмного забезпечення системи управління; $V(r,t)$ – функція, яка характеризує швидкісні характеристики системи управління; $T(t)$ – функція, яка характеризує часові параметри системи управління.

Таким чином задача синтезувати самовідновлювальну систему управління полягає в розробці методів та алгоритмів, максимізуючий функціонал виду (1). Математично це можна виразити через цільову функцію $\gamma(x)$, яка записується у вигляді

$$\gamma(\mathrm{x}) = \max F\left(G(h,r),I(R),S(L),V(r,t),T(t)\right). \qquad (2)$$

При цьому повинні виконуватися такі обмеження:

$$\begin{gathered} G(h,r) \ge g_{доп},\ I(R) \le I_{доп},\ S(L) \ge S_{доп}, \\ V(r,t) \le V_{доп},\quad T(t) \le T_{доп}, \end{gathered} \qquad (3)$$

де $g_{доп}$ – мінімально допустиме значення енергетичних параметрів системи управління; $I_{доп}$ – необхідне значення стійкості від зовнішніх впливів; $S_{доп}$ - задане значення структурної надійності програмного забезпечення системи управління; $V_{доп}$ - мінімально допустиме значення швидкісних характеристик системи управління; $T_{доп}$ - максимально допустимий час для виконання команд управління.

Таким чином, вираз (2) з урахуванням обмежень (3), в узагальненому вигляді описує основну задачу досліджень – синтез системи управління, забезпечуючи в комплексі максимальну якість системи управління при заданих ймовірнісно-часових характеристик, в умовах впливу потужних засобів боротьби.

Проведені дослідження показали [11], що задача синтезу, забезпечуючих умов (2) при обмеження їх (3) являється екстремальною задачею. Варіаційний характер задачі побудови самовідновлювальної системи управління вбачає використання в якості математичного програмування ідей і методів функціонального аналізу, теорії оптимального управління, чисельні методи оптимізації, алгебраїчні методи синтезу та аналізу дискретних систем, що включає теоретико-числові та комбіновано-множинні методи.

Важкість задачі синтезу системи управління, що забезпечують умову (2) пояснюються, по-перше, взаємним зв'язком аргументів, що входять в функцію вигляду (1), по-друге, широким спектром вихідних обмежень, характеризуючих особливості функціонування системи управління.

Основним визначальним джерелом появи інформаційних ризиків є інформаційний актив, до яких належить будь-яка інформація, що становить цінність для організації. Робота з мінімізації ІТ-ризиків полягає у попередженні несанкціонованого доступу до активів, аварій та збоїв обладнання, забезпеченні доступності необхідних для роботи сервісів та додатків. Процес мінімізації інформаційних ризиків слід розглядати комплексно: спочатку виявляються можливі проблеми, а потім визначається, якими способами їх можна вирішити чи попередити.

Класифікація ризиків означає об'єднання сукупності ризиків на підставі певних ознак та критеріїв. Такими критеріями, покладеними в основу класифікації інформаційних ризиків, можуть бути критерії, наведені на рис. 1.

Рис. 1. Класифікація інформаційних ризиків

Для вирішення оптимізаційних завдань, пов'язаних з вибором параметрів систем управління та алгоритмів функціонування системи, з метою мінімізації ризику застосовується апарат теорії ігор. Ігровий підхід пропонує кожному гравцю дії, розраховані на найменш вигідну для нього реакцію супротивника. До кількості завдань, що легко перекладаються мовою теорії ігор, відноситься й синтез алгоритмів функціонування системи управління в умовах конфлікту між системою управління і протидіючою стороною за умови забезпечення гарантованих ймовірнісно-часових показників системи.

У термінах теорії ігор подібна ситуація адекватна вибору двома гравцями найкращих стратегій з множини всіх можливих на основі деякого середнього показника якості $\overline{y}$.

Нехай пропонується заданим, з одного боку, апріорний алфавіт можливих станів системи управління A і ймовірність їхнього створення

$$P = p(P_{00}, P_{01}, \ldots, P_{0m}, P_{12} \ldots, P_{N0}, P_{N1}, \ldots P_{NN}),$$

з іншого – різні стратегії протидії й типи використовуваних загроз S і ймовірності їхнього створення

$$Q = q\left(q_{ij}\right), \quad i = \overline{1,M},\ j = \overline{1,J}\ .$$

Тоді матриця гри описується табл. 1, де y_{ij}^{kc} – частковий показник якості застосування алгоритму функціонування системи управління й використання j-го класу сигнально алгоритму функціонування при k-й стратегії протидії i-ї ризику.

Таблиця 1 – **Матриця гри**

Алгоритм функціонування		Імовірності	Стратегії противника			
			S_0	S_1	…	S_m
			Q_0	Q_1	…	Q_m
			$q_{00}, q_{01}, \ldots q_{0L}$	$q_{10}, \ldots q_{l0}$	…	$q_{0}, \ldots q_{Mq}$
		P_{00}	$\acute{o}_{00}^{00}, \acute{o}_{10}^{00} \ldots \acute{o}_{l0}^{00}$	…	…	$\acute{o}_{00}^{m0} \ldots \acute{o}_{q0}^{m0}$
		P_{01}	$\acute{o}_{01}^{00}, \acute{o}_{11}^{00} \ldots \acute{o}_{i1}^{00}$	…	…	$\acute{o}_{01}^{m0} \ldots \acute{o}_{q1}^{m0}$
A_0	P_0	…	…	…	…	…
		P_{0m}	$\acute{o}_{0m}^{00}, \acute{o}_{1m}^{00} \ldots \acute{o}_{im}^{00}$	$\acute{o}_{0m}^{10} \ldots \acute{o}_{bm}^{10}$		$\acute{o}_{0m}^{m0} \ldots \acute{o}_{qm}^{m0}$
…	…	…	…	…	…	…
A_l	P_l	P_{l0}	$\acute{o}_{00}^{0l}, \acute{o}_{10}^{0l} \ldots \acute{o}_{l0}^{0l}$	$\acute{o}_{10}^{1l} \ldots \acute{o}_{b0}^{1l}$		$\acute{o}_{00}^{ml} \ldots \acute{o}_{q0}^{ml}$
		…	…	…	…	…
A_N	P_N	P_{N0}	$\acute{o}_{00}^{0N}, \acute{o}_{10}^{0N} \ldots \acute{o}_{l0}^{0N}$	$\acute{o}_{10}^{1N} \ldots \acute{o}_{b0}^{1N}$		$\acute{o}_{00}^{mN} \ldots \acute{o}_{q0}^{mN}$
		…	…	…	…	…
		P_{Nc}	$\acute{o}_{0z}^{0N}, \acute{o}_{1z}^{0N} \ldots \acute{o}_{iz}^{0N}$	$\acute{o}_{1z}^{1N} \ldots \acute{o}_{bz}^{1N}$		$\acute{o}_{0z}^{mN} \ldots \acute{o}_{qz}^{mN}$

Аналіз концепції протидії противника показує, що даний конфлікт є нерозв'язним у чистих концепціях.

Нехай система управління застосовує змішані стратегії, тобто змінює алгоритм функціонування або клас використовуваних стратегій, що задані на множині $\{A\}$. Отже, показником якості в цьому випадку буде результат усереднення за всіма частковими показниками.

Противник може здійснювати вибір перешкоди як без оцінки результатів впливу на систему управління, так і з оцінкою впливу. Спочатку припустимо, що противник здійснює вибір стратегії подавлення системи управління без урахування їх впливу на систему. У цьому випадку система управління може реалізувати такі стратегії поведінки в конфліктній ситуації:

– система управління не змінює алгоритм функціонування, але змінює клас використовуваних алгоритмів функціонування таким чином, щоб досягти максимального значення середнього показника якості вибором імовірності P_{ij} при заданому наборі стратегій протидії;

– система управління змінює алгоритм функціонування, клас використовуваних алгоритмів функціонування з метою максимізації середнього показника якості при фіксованих стратегіях протидії;

– система управління змінює алгоритм функціонування й клас використовуваних алгоритмів функціонування залежно від стратегії протидії з метою

досягнення максимального значення часткового показника якості.

Твердження 1. Нехай у системі управління реалізується A_i стратегія функціонування з i-м алгоритмів функціонування. Причому система управління не змінює алгоритм функціонування. Тоді середнє значення показника якості визначається виразом

$$\bar{y} = \sum_{j=0}^{m} \sum_{z=0}^{R_j} Q_j q_{jr} y_r^i R^i , \qquad (4)$$

де R_j залежно від j дорівнює $l, b, \ldots, q...$

Твердження 2. Нехай у системі управління реалізується A_i стратегія функціонування. У процесі функціонування, залежно від стратегії протидії, клас використовуваних алгоритмів функціонування змінюється. Тоді середнє значення показника якості визначається виразом

$$\bar{y} = \max_{Pic \in P_i} \sum_{c=0}^{z_i} \left(\sum_{j=0}^{m} \sum_{r=0}^{R_j} Q_j q_{jz} y_{rc}^{ji} \right) P_{ic} P_i , \qquad (5)$$

де z_i дорівнює $m, \ldots Z$ залежно від i .

Твердження 3. Нехай система управління змінює алгоритм функціонування з метою максимізації середнього показника якості при фіксованих стратегіях протидії. Тоді середнє значення показника якості визначається виразом:

$$\bar{y} = \sum_{i=v}^{N} \left\{ \max_{Pic \in P_i} \sum_{c=0}^{z_i} \left(\sum_{j=0}^{m} \sum_{r=0}^{R_j} Q_j q_{jR} y_{ri}^{ji} \right) P_{ic} P_i \right\}. \qquad (6)$$

Твердження 4. Нехай система управління змінює алгоритм функціонування залежно від стратегій протидії з метою максимізації значення часткового показника якості. Тоді середнє значення показника якості визначається виразом:

$$\bar{y} = \sum_{j=0}^{m} \sum_{z=0}^{R_j} Q_j q_{jr} \left\{ \begin{array}{l} \left[P_i^* P_{i*} C^* \max_{i \in N} \left(y_{rc}^{ji} \right) \right] + \\ + \sum_{i=0, i \neq i^* c \neq c^*}^{c=0} P_i P_{io} y_{zc}^{ji} \end{array} \right\}, \qquad (7)$$

де P_i^* й $P_{i*}C^*$ – ймовірності використання i-стратегії і C- алгоритм функціонування системи управління, що мають максимальне значення часткового показника y_{rc}^{ji} при впливі j-ї стратегії протидії й r -ї алгоритму.

При виборі супротивником стратегій протидії з урахуванням оцінки їх впливу на систему управління за умови максимального її подавлення можуть використовуватися ті ж стратегії поведінки системи управління в конфліктній ситуації, що і в першому випадку. Варто врахувати, що супротивник вибирає стратегію подавлення, за якої показник якості функціонування має мінімальне значення.

З використанням апарата теорії ігор проведений аналіз і розроблена методика оцінки середнього значення показника якості функціонування системи зв'язку при різних стратегіях конфліктуючих сторін.

Проведені дослідження дозволили отримати вирази для оцінки середнього значення якості функціонування системи управління при різних стратегіях поведінки й оцінки впливу протидії.

Визначимо межі зміни середнього показника якості функціонування системи зв'язку при впливі завад. Позначаючи через $\overline{y_{зад}}$ задане значення середнього показника якості функціонування системи зв'язку й управління в умовах протидії, отримуємо межі зміни $\bar{y}$.

При протидії без оцінки результатів впливу завад відповідно до тверджень 1 й 4:

$$\begin{array}{l} \bar{y} = \sum_{j=0}^{m} \sum_{z=0}^{R_j} Q_j q_{jr} \left\{ \left[P_i^* c^* \max_{i \in r} \left(y_{rc}^{ji} \right) \right] + \right. \\ \left. + \sum_{i=0}^{N} \sum_{c=0}^{Z_i} P_i P_{ic} \overline{y_{rc}^{-ij}} \geq \overline{y_{зад}} > \sum_{j=0}^{m} \sum_{z=0}^{R_j} Q_j q_{jr} y_{rc}^{ji} \right\}, \end{array} \qquad (8)$$

При виборі стратегії протидії:

$$\begin{array}{l} \bar{y} = Q_j^* q_j^* r^* P_i^* p_i^* c \min_{j \in m} \left(m_j \right) \max_{i \in N} \left(N_i y_{r^* c^*}^{ji} \right) + \\ + \sum_{j=0}^{m} \sum_{r=0}^{R_i} Q_i q_{jr} \times \sum_{m}^{N} \sum_{R_i}^{r_i} P_i P_{ic} y_{rc}^{ij} \geq \overline{y_{зад}} > \\ > Q_j \left\{ q_{jr^*} \min_{r \in R} \left(y_{r^* c} \right) \right\} + \sum_{j=0}^{m} \sum_{z=0}^{R_i} Q_j y^{ij} . \end{array} \qquad (9)$$

Висновки

Таким чином розв'язання завдання підвищення якості функціонування системи управління можливе за рахунок:

–застосування змішаної стратегії поведінки системи управління;

–вибору структури і параметрів системи управління, що збільшують часткові показники якості її функціонування;

–збільшення ймовірності розпізнавання діючої стратегії подавлення і класу алгоритмів функціонування та зміни алгоритму функціонування системи управління.

СПИСОК ЛІТЕРАТУРИ

1. Найт Ф. Понятие риска и неопределенности. *Теория и история экономических и социальных институтов и систем*. 1994. № 5. С. 22-29.
2. Менеджмент качества [Электронный ресурс]. URL: http://www.kpms.ru/Automatization
3. Управление рисками на предприятии [Электронный ресурс]. URL: http://www.risk24.ru/
4. Активы организации как ключевые факторы риска [Электронный ресурс]. URL: https://www2.deloitte.com/content
5. Берлимер Б. Риски в современном бизнесе. М.: Аланс, 1994. 200 с.
6. Suroso, J. S, & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution, 3rd Inte. Conf. on Computer Science and Computational Intelligence, 135, pp. 202-213.

7. Suroso, J. S., Rahadi, B. (2017). Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy. ACM International Conference Proceeding Series. Part F130654.
8. Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности. *Вестник НГУ. Серия: Информационные технологии*, 2011. Т. 9, вып/ 2. С. 80-89.
9. Datta, S. P. (2010). Risk Management Process for Information Security System. International Journal of Computer Science andCommunication, 1(1), 33-38.
10. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27.
11. Покровский, П. Оценка информационных рисков. *LAN*. 2010. № 10. С/ 25-31/

Received (Надійшла) 26.08.2021
Accepted for publication (Прийнята до друку) 10.11.2021

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Лебедєв Олег Григорович – кандидат технічних наук, доцент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Oleh Lebediev – Candidate of Technical Sciences, Associate Professor of Electronic Computers Department, National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: oleh.lebediev@nure.ua; ORCID ID: https://orcid.org/0000-0001-5998-0136

Лебедєв Валентин Олегович – аспірант кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Valentyn Lebediev – postgraduate student of Electronic Computers Department, National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: valentyn.lebediev@nure.ua; ORCID ID: https://orcid.org/0000-0002-0095-7481

Методика анализа рисков в информационных системах

О. Г. Лебедев, В. О. Лебедев

Аннотация. Разрабатывается методика анализа рисков в информационных системах. Исследуются пути обеспечения эффективности функционирования систем управления в условиях информационного противоборства с использованием аппарата теории игр. Стремление обеспечить высокую эффективность современных информационных комплексов управления, минимизировать финансовые затраты, обеспечить энергетическую и информационную защиту системы управления, выдвигает на первый план создание системы анализа и управления рисками в информационных системах. Предполагается, что система управления может реализовать следующие стратегии поведения в конфликтной ситуации: система управления не изменяет алгоритм функционирования, но изменяет класс используемых алгоритмов функционирования таким образом, чтобы добиться максимального значения среднего показателя качества выбором вероятности P_{ij} при заданном наборе стратегий противодействия, система управления изменяет алгоритм функционирования, класс используемых алгоритмов функционирования с целью максимизации среднего показателя качества при фиксированных стратегиях противодействия, система управления изменяет алгоритм функционирования и класс используемых алгоритмов функционирования в зависимости от стратегии противодействия с целью достижения максимального значения качества. С использованием аппарата теории игр проведен анализ и разработана методика оценки среднего значения показателя качества функционирования системы связи при разных стратегиях конфликтующих сторон. Разрабатывается методика оценки среднего значения показателя свойства функционирования системы управления и полученные выражения для оценки среднего значения показателя при разных стратегиях поведения. Показано, что решение проблемы повышения качества функционирования системы управления возможно за счет применения смешанной стратегии поведения системы, выбора структуры и параметров системы управления, увеличивающих частные показатели качества ее функционирования.

Ключевые слова: анализ рисков; информационные системы; системы управления; самовосстанавливающаяся система; угрозы информации; синтез системы.

Analysis of risks methodology in information systems

Oleh Lebediev, Valentyn Lebediev

Abstract. A method of risk analysis in information systems is being developed. The ways of ensuring the efficiency of control systems in the conditions of information confrontation with the use of the game theory apparatus are investigated. The desire to ensure high efficiency of modern management information systems, minimize financial costs, provide energy and information protection of the management system, highlights the creation of a system of analysis and risk management in information systems. It is assumed that the control system can implement the following behavioral strategies in a conflict situation: the control system does not change the algorithm, but changes the class of algorithms used to achieve the maximum value of the average quality by choosing the probability P_{ij} for a given set of countermeasures, the control system changes the algorithm operation, the class of operating algorithms used to maximize the average quality of fixed countermeasures, the control system changes the operating algorithm and the class of operating algorithms used depending on the countermeasure strategy in order to achieve maximum quality. Using the apparatus of game theory, an analysis was performed and a method for estimating the average value of the quality of the communication system with different strategies of the conflicting parties was developed. The technique of estimation of average value of an indicator of quality of functioning of a control system is developed and expressions for an estimation of average value of an indicator at various strategies of behavior are received. It is shown that the solution to the problem of improving the quality of the control system is possible through the use of a mixed strategy of system behavior and the choice of structure and parameters of the control system that increase the partial quality of its operation.

Keywords: risk analysis; information systems; control systems; self-healing system; information threats; synthesis systems.