
INFORMATION SECURITY RISK MANAGEMENT

УДК 004.056.53

ЄВГЕН МАКСИМЕНКО,
ВАСИЛЬ ЦУРКАН,
ЯРОСЛАВ ДОРОГИЙ,
ОЛЬГА КРУК**ОЦІНЮВАННЯ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЇ НА ОСНОВІ СПЕКТРАЛЬНОГО ПІДХОДУ**

Розглядається використання систем менеджовування безпекою інформації за результатами оцінювання ризику. Для цього через заплановані інтервали часу накопичуються статистичні дані про загрози та збитки внаслідок їх реалізації. Як наслідок, створюються передумови для використання статистичного підходу. Однак, цей підхід до оцінювання ризику обмежується високими вимогами до обсягу статистичних даних, завищенням оцінок ризику, складністю врахування коливань величини збитку, відсутністю єдиного еталону при зіставленні ризиків. Для подолання означених обмежень пропонується спектральний підхід до оцінювання ризику в системах менеджовування безпекою інформації. Визначаються умови його використання, зокрема: накопичення статистичних даних про загрози та збитки внаслідок їх реалізації, врахування динаміки ризику, встановлення еталону для порівняння ризиків.

Ключові слова: безпека інформації, ризик, сигнал ризику безпеки інформації, оцінювання ризику, спектральний підхід, система менеджовування безпекою інформації.

Постановка проблеми у загальному вигляді. Розроблення та впровадження системи менеджовування безпекою інформації є стратегічним рішенням для організації. Його прийняття дозволяє забезпечити збереження конфіденційності, цілісності та доступності інформації при використанні означених систем. Це досягається шляхом оцінювання ризику через заплановані інтервали часу на основі накопичення статистичних даних про загрози та збитки внаслідок їх реалізації [1-5].

Аналіз останніх досліджень і публікацій. Підходи до оцінювання ризиків досліджуються в [4-13]. Зокрема, за наявності статистичних даних рекомендується використовувати статистичний підхід [4-11]. Він орієнтований на оцінювання ризику безпеки інформації за допомогою ймовірності нанесення збитку та показників його варіації, наприклад [4, 5, 12]: дисперсії, середньоквадратичного відхилення або коефіцієнта варіації. Цими показниками характеризується зміна величини збитку навколо середнього значення без урахування динаміки її поведінки (різких, неупорядкованих коливань [12]). Однак, використання такого підходу обмежується високими вимогами до обсягу статистичних даних і, як наслідок, можливістю встановлення закону розподілення величини збитку; завищенням оцінок ризику за показниками варіації; складністю врахування коливань величини збитку [5, 12, 13]. Крім цього, складністю зіставлення оцінок ризиків різноманітної природи через відсутність єдиного еталону [13]. Подолання означених обмежень можливе шляхом використання спектрального підходу до оцінювання ризиків [12-20] та ризику безпеки інформації, зокрема [21, 22].

Тому **метою статті** є аналізування спектрального підходу до оцінювання ризику безпеки інформації для встановлення умов та обмежень його використання.

Виклад основного матеріалу дослідження. При використанні спектрального підходу процес оцінювання ризику безпеки інформації зводиться до оцінювання його сигналу [12-20].

Цей сигнал визначається як випадковий процес, відліками якого є відхилення величини збитку від очікуваного значення, та формалізується виразом [12-14]

$$s(t) = x(t) - x_0(t), \quad (1)$$

де $s(t)$ – сигнал ризику (див., наприклад [12, 14], рис. 1);

$x(t)$ і $x_0(t)$ – отримане та очікуване значення величини збитку;

t – час.

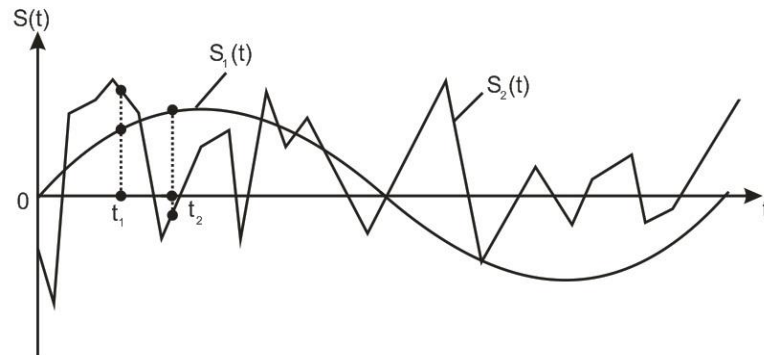


Рисунок 1 – Приклад реалізацій $s_1(t)$ і $s_2(t)$ сигналу ризику

З огляду на рис. 1, сигнал ризику спостерігається протягом певного проміжку часу та представляється послідовністю значень $s(t_i)$ у окремі моменти часу $t_1, t_2, \dots, t_i, \dots, t_n$. Ця послідовність відображається часовим рядом випадкових величин $S_1, S_2, \dots, S_i, \dots, S_n$ (див. наприклад [14], рис. 2), що відповідають перетинам сигналу ризику $s(t_1), s(t_2), \dots, s(t_i), \dots, s(t_n)$.

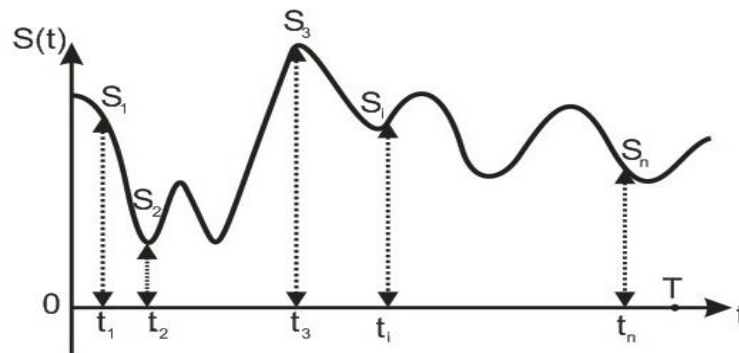


Рисунок 2 – Приклад відображення сигналу ризику часовим рядом

Завдяки цьому він описується n мірним законом розподілення, $p(S_1, S_2, \dots, S_i, \dots, S_n; t_1, t_2, \dots, t_i, \dots, t_n)$. Проте його використання на практиці для оцінювання сигналу ризику ускладнене [12, 14]. Тому обмежуються визначенням математичного очікування, дисперсії, середньоквадратичного відхилення. Таке визначення стало можливим завдяки відображенню сигналу ризику його значеннями S_i у моменти часу t_i , а саме [12-14]:

1. Математичне очікування $M[S_i]$

$$M[S_i] = \int_0^{+\infty} S_i \cdot p(S_i; t_i) dS_i, \quad (2)$$

де $p(S_i, t_i)$ – одномірний закон розподілення випадкової величини S_i в момент часу t_i .

2. Дисперсія $D[S_i]$

$$D[S_i] = M[(S_i - M[S_i])^2] = \int_0^{+\infty} (S_i - M[S_i])^2 \cdot p(S_i; t_i) dS_i, \quad (3)$$

3. Середньоквадратичне відхилення $\sigma[S_i]$

$$\sigma[S_i] = \sqrt{D[S_i]}. \quad (4)$$

Використання (1)-(4) дозволяє визначити діапазон з реалізаціями сигналу ризику без урахування їх поведінки всередині нього. Це призводить до складнощів визначення ступеня мінливості сигналу в залежності від зміни часу. Для охарактеризування такої залежності в моменти часу t_i та t_{i+1} використовується кореляційна функція. Вона дозволяє оцінити статистичний зв'язок миттєвих значень сигналу ризику в різні моменти часу.

Наприклад, при $i = 1$ отримаємо [12, 19]

$$k(S_1, S_2) = M[\overset{\circ}{S}_1, \overset{\circ}{S}_2], \quad (5)$$

де $k(S_1, S_2)$ – кореляційна функція в моменти часу t_1 та t_2 ;

$\overset{\circ}{S}_1$ і $\overset{\circ}{S}_2$ – центроване значення сигналу ризику в моменти часу t_1 та t_2

$$\overset{\circ}{S}_1 = S_1 - M[S_1], \quad \overset{\circ}{S}_2 = S_2 - M[S_2].$$

Водночас зв'язок між значеннями сигналу ризику може характеризуватися нормованою кореляційною функцією або коефіцієнтом кореляції [12]

$$\rho(S_1, S_2) = \frac{k(S_1, S_2)}{\sqrt{\sigma^2(S_1) + \sigma^2(S_2)}}. \quad (6)$$

Крім показників кореляції (5)-(6) для оцінювання сигналу ризику здійснюється його відображення комбінацією простих складових за впорядкованою системою ортогональних функцій. Серед різноманітних систем, простотою обчислень характеризуються тригонометричні форми ряду Фур'є. В цьому випадку спектральне представлення сигналу ризику є розкладанням на суму елементарних гармонічних коливань з різними частотними складовими $\omega_1, \omega_2, \dots, \omega_i, \dots, \omega_n$, наприклад [12, 14, 19]:

$$s(t) = \sum_{j=0}^{\infty} (U_j \cos \omega_j t + V_j \sin \omega_j t),$$

де U_j, V_j – амплітуди елементарних гармонічних коливань, що є випадковими величинами та тлумачаться як коефіцієнти Фур'є.

У результаті такого розкладання отримується енергетичний спектр та, як наслідок, встановлюється залежність між сигналом ризику в часовій та спектральних областях. При цьому, енергетичним спектром або спектральною щільністю потужності $F(\omega)$ називається функція (див., наприклад [14], рис. 3), якою описується розподілення середньої потужності сигналу ризику в залежності від зміни частоти ω .

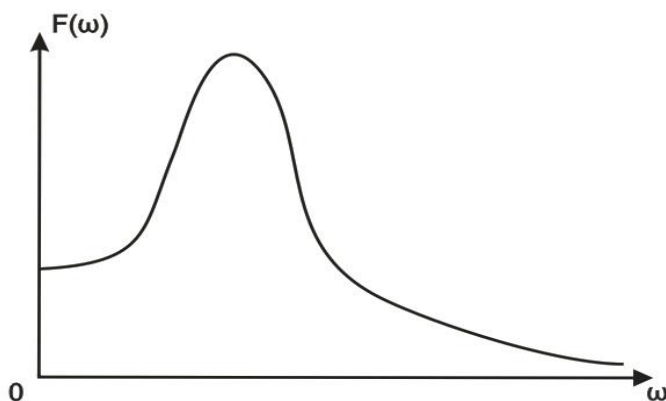


Рисунок 3 – Приклад відображення енергетичного спектру сигналу ризику

Завдяки цьому визначається щільність розподілення середніх потужностей окремих гармонік за частотним спектром і, як наслідок, встановлюються характер коливань і внутрішня структура сигналу ризику. Зокрема [19], чим вища потужність окремих ділянок енергетичного спектру, тим більший їх вклад у відхилення величини збитку. Низькочастотні складові спектру відповідають за повільну, плавну зміну її значення, а високочастотні – швидкі та різкі коливання. Як наслідок, чим більше високочастотних складових в енергетичному спектрі сигналу ризику, тим менш передбачувана поведінка величини збитку. Завдяки цьому за формою енергетичного спектру визначається внутрішня структура та поведінка сигналу ризику, а також встановлюється тісний та глибокий зв'язок між його часовими та спектральними властивостями [12-14, 19, 20].

На основі цих тверджень у [14] визначаються як основні характеристики сигналу ризику закон розподілення величини збитку та спектральне розподілення потужності. Першою характеристикою оцінюється перебування сигналу ризику в певному інтервалі часу, відношення максимальних значень до середньоквадратичних. Тоді як другою – розподілення середньої потужності за частотами. При цьому сигнал з постійним енергетичним спектром визначається як білий шум, що характеризується некорельованими миттєвими значеннями. Це вказує на необмежено велику швидкість їх зміни, що призводить до поведінки білого шуму з максимальною невизначеністю та ризиком. Цю особливість взято за основу для визначення еталону порівняння та класифікування ризиків різної природи між собою. Використання такого еталону дозволило порівнювати енергетичні спектри сигналів ризику з рівномірним спектром білого шуму та у разі їх співпадання стверджувати про максимальний ризик [12-20]. Завдяки такому порівнянню можна враховувати характер поведінки величини збитку та оцінювати ризик безпеки інформації.

Представлення абстрактної моделі сигналу ризику білим шумом характеризується максимальним ризиком [14]. Тоді для будь-якого сигналу ризику справедлива така нерівність

$$r \leq r_b,$$

де r_b – оцінка ризику для білого шуму, $r_b = 1$ або $r_{b,\%} = 100$;

r – оцінка ризику для будь-якого сигналу.

У цьому випадку мірою ризику є розбіжність між енергетичним спектром білого шуму та сигналу ризику, використання якої дозволяє оцінити [20]:

- імовірні коливання величини збитку;
- невизначеність (непередбачуваність) величини збитку.

Для цього вводиться спектральний показник ризику, компонентами якого є означені окремі показники. Внаслідок цього, отримаємо таку мультиплікативну модель для оцінювання ризику [13, 14, 20]

$$r_{\%} = (r_p \times r_f) \times 100, 0 \leq r \leq r_{b,\%}, \quad (7)$$

де r_p – окремий показник ризику для оцінювання ймовірних коливань величини збитку, що враховує розбіжності потужності сигналу ризику та білого шуму;

r_f – окремий показник для оцінювання невизначеності величини збитку, що враховує її поведінку та залежить від форми енергетичного спектру.

Окремі показники r_p і r_f ризику визначаються як нормовані значення відповідних «натуральних» показників [15]

$$r_p = \frac{V_x}{V_b}; \quad r_f = \frac{k_x}{k_b},$$

де V_x і V_b – коефіцієнти варіації величини збитку та еталонного білого шуму

$$V_x = 1, V_b = 1 \rightarrow r_p = 1; \quad (8)$$

k_x і k_b – коефіцієнти оцінювання форми енергетичного спектру сигналу ризику з еталонним білим шумом.

$$k_x = 1, k_b = 1 \rightarrow r_f = 1. \quad (9)$$

Шляхом підстановки (8) і (9) в (7) отримаємо оцінку ризику для білого шуму

$$r_{\%} = 100\%.$$

При цьому, оцінка ризику (7) буде рівною нулю за рівності нулю одного з окремих показників r_p або r_f . Окремий показник r_p рівний нулю за відсутності випадкової складової у величини збитку, $V_x = 0$. Інший показник r_f прямує до нуля, якщо енергетичний спектр сигналу ризику складається з однієї гармоніки, що передбачається з огляду на подальшу її поведінку [14, 15].

Таким чином, використання спектрального підходу до оцінювання ризику безпеки інформації супроводжується такими можливостями [19, 20]:

1. Дослідження та врахування вкладу окремих спектральних гармонік шляхом визначення внутрішньої структури сигналу ризику.

2. Підвищення точності оцінювання сигналу ризику завдяки частковому компенсуванню потужностей окремих гармонік енергетичного спектру.

3. Врахування характеру поведінки величини збитку шляхом дослідження розбіжностей у формах сигналу ризику та білого шуму.

4. Оцінювання максимально можливого коливання величини збитку, перевищення чи не перевищення порогового значення, кількість його перевищень, вихід величини збитку за встановленні межі.

5. Використання мір невизначеності та передбачуваності величини збитку для оцінювання ризику.

6. Використання форми енергетичного спектру для класифікування ризиків різної природи.

7. Оцінювання ризику за відсутності закону розподілення величини збитку.

8. Оцінювання ризику за обмеженого обсягу статистичних даних про загрози та збитки внаслідок їх реалізації.

9. Обробляння ризику з випередженням за його оцінками з прогнозним значення величини збитку.

10. Використання єдиного еталону для оцінювання та порівняння ризиків різної природи.

Висновки. Спектральний підхід до оцінювання ризику безпеки інформації орієнтований на подолання характерних обмежень для статистичного підходу. За його основу взято дослідження енергетичного спектру сигналу ризику при інтегральному перетворенні Фур'є та його порівняння зі встановленим еталоном. Завдяки цьому стало можливим оцінювання як імовірного відхилення величини збитку від очікуваного значення, так і її невизначеності (непередбачуваності).

Разом з тим, використанню спектрального підходу передують виконання таких умов та обмежень:

1. Накопичення статистичних даних про збитки внаслідок реалізації загроз за встановлений інтервал часу для оцінювання як імовірнісних, так і часових та спектральних характеристик ризику.

2. Врахування динаміки зміни ризику шляхом його відображення *ергодичним, стаціонарним* сигналом ризику, дослідження якого дозволить оцінити притаманні йому властивості та характеристики.

3. Встановлення еталонного прийняттого рівня ризику для порівняння визначених оцінок його величини. Цим забезпечується зіставність отриманих результатів при атестуванні ризику та, як наслідок, можливість обробляння неприйнятних оцінок.

Як наслідок, складно стверджувати про необхідність чи достатність означеного переліку умов використання спектрального підходу. Це обумовлено, перш за все, нестационарністю сфери безпеки інформації. Тому тільки за результатами дослідження сигналу ризику можна стверджувати або спростовувати адекватність такого відображення та можливість використання спектрального підходу до оцінювання ризику безпеки інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.
2. Information technology. Security techniques. Information security incident management : ISO/IEC 27035:2011. – Second edition 2013-09-01. – Geneva, 2011. – P. 78.
3. Information technology. Security techniques. Information security risk management: BS ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – P. 68.
4. Буянов В. П. Рискология (управление рисками) : учеб. пособие. – 2-е изд. / В. П. Буянов, К. А. Кирсанов, Л. М. Михайлов. – М. : Издательство «Экзамен», 2003. – 384 с.
5. Вишняков Я. Д. Общая теория рисков : учеб. пособие для студ. высш. учеб. заведений / Я. Д. Вишняков, Н. Н. Радаев. – М. : Издательский центр «Академия», 2007. – 368 с.
6. Risk management. Risk assessment techniques : IEC 31010:2009. – Second edition 2009-11-01. – Geneva, 2009. – P. 176.
7. Акимов В. А. Риски в природе, техносфере, обществе и экономике / В. А. Акимов, В. В. Лесных, Н. Н. Радаев; МЧС России. – М. : Деловой экспресс, 2004. – 352 с.
8. Вітлінський В. В. Ризикологія в економіці та підприємстві : монографія / В. В. Вітлінський, Г. І. Великоіваненко. – К. : КНЕУ, 2004. – 480 с.
9. Качинський А. Б. Безпека загрози і ризик : наукові концепції та математичні моделі / А. Б. Качинський. – К., 2003. – 472.
10. Лисиченко Г. В. Природний, техногенний та екологічний ризики : аналіз, оцінка, управління / Г. В. Лисиченко, Ю. Л. Забулонов, Г. А. Хміль. – К. : Видавництво «Наукова думка», 2008. – 544 с.
11. Ступаков В. С. Риск-менеджмент / В. С. Ступаков, Г. С. Токаренко. – М. : Издательство «Финансы и статистика», 2006. – 288 с.
12. Матвеев Б. А. Спектральный метод оценки и прогнозирования статистических рисков : монография / Б. А. Матвеев. – Челябинск : Изд-во ЮУрГУ, 2007. – 85 с.
13. Матвеев Б. А. Теоретические основы исследования статистических рисков : монография / Б. А. Матвеев. – Челябинск : Изд-во ЮУрГУ, 2008. – 248 с.
14. Матвеев Б. А. Сигнал риска и его характеристики / Б. А. Матвеев, Л. С. Сосненко // Управление риском. – 2009. – № 1 (49). – С. 2-8.
15. Матвеев Б. А. Спектральный показатель экономического риска [Электронный ресурс] / Б. А. Матвеев. – Режим доступа : <http://dspace.susu.ac.ru/handle/0001.74/1419>. – Дата доступа : сентябрь 2015. – Название с экрана.
16. Матвеев Б. А. Прогнозирование экономического результата и связанного с ним риска / Б. А. Матвеев // Вестник Южно-Уральского государственного университета. – 2011. – № 21 (238). – С. 54-58.
17. Матвеев Б. А. Спектральный подход к анализу и измерению риска / Б. А. Матвеев // Проблемы анализа риска. – 2012. – Том 9, № 2. – С. 68-75.
18. Сосненко Л. С. Спектральный показатель качества экономической модели / Л. С. Сосненко, Б. А. Матвеев // Вестник Челябинского государственного университета. Экономика. – 2013. – № 32 (323). – Экономика, вып. 42. – С. 5-9.
19. Матвеев Б. А. Спектральная теория рисков / Б. А. Матвеев // Вестник Южно-Уральского государственного университета. – 2014. – Том 8, № 2. – С. 20-24.
20. Матвеев Б. А. Основы спектральной теории рисков / Б. А. Матвеев // Управление риском. – 2015. – № 2. – С. 3-6.
21. Мохор В. В. Оцінювання ризику безпеки інформації на основі спектрального підходу / В. В. Мохор, Є. В. Максименко, Я. В. Зінченко, В. В. Цуркан // Безпека інформації в інформаційно-телекомунікаційних системах (26-28 травня 2015 р.) : XVII міжн. наук.-практ. конф. : тези доп. – К. : Видавництво ДССЗЗІ України, 2015. – С. 70.
22. Мохор В. В. Умови використання спектрального підходу для оцінювання ризику безпеки інформації / В. В. Мохор, Є. В. Максименко, Я. В. Зінченко, В. В. Цуркан // Стан та удосконалення

безпеки інформаційно-телекомунікаційних систем (09-12 червня 2015 р.) : 7 Всеукр. наук.-практ. конф. : тези доп. – Миколаїв-Коблево : ТОВ «Ділова інформація», 2015. – С. 72.

Стаття надійшла до редакції 22.10.2015.

REFERENCE

1. International Organization for Standardization (2013), ISO/IEC 27001:2013, *Information technology. Security techniques. Information security management systems. Requirements*, Geneva, 23 p.
2. International Organization for Standardization (2011), ISO/IEC 27035:2011, *Information technology. Security techniques. Information security incident management*, Geneva, 78 p.
3. International Organization for Standardization (2011), BS ISO/IEC 27005:2011, *Information technology. Security techniques. Information security risk management*, Geneva, 68 p.
4. Buianov, V. P., Kirsanov, K. A., Mikhailov, L. M. (2003), *Riskologiya (upravlenie riskami)* [Riskology (risk management)], Ekzamen Publ., Moscow, 384 p.
5. Vishniakov, Y. D., Radaev, N. N. (2007), *Obshchaia teoriia riskov* [General risk theory], Akademiia Publ., Moscow, 368 p.
6. International Organization for Standardization (2009), IEC 31010:2009, *Risk management. Risk assessment techniques*, Geneva, 176 p.
7. Akimov, V. A., Lesnykh, V. V., Radaev, N. N. (2004), *Riski v prirode tekhnosfere obshchestve i ekonomike* [Risks in nature, technosphere, society and economics], Delovoi ekspres Publ., Moscow, 352 p.
8. Vitlinskyi, V. V., Velykoivanenko, H. I. (2004), *Ryzykologiya v ekonomitsi ta pidpriemnytstvi* [Riskology in economics and business], KNEU Publ., Kyiv, 480 p.
9. Kachynskyi, A. B. (2003), *Bezpeka, zahrozy i ryzyk : naukovy kontseptsii ta matematychni modeli* [Security, threats and risk : scientific concepts and mathematical models], Kyiv, 472 p.
10. Lysychenko, H. V., Zabulonov, Y. L., Khmil, H. A. (2008), *Pryrodnyi, tekhnohennyi ta ekolohichni ryzyky : analiz, otsinka, upravlinnia* [Natural, technological and environmental risk : analysis, assessment, management], Naukova dumka Publ., Kyiv, 544 p.
11. Stupakov, V. S., Tokarenko, G. S. (2006), *Risk-menedzhment* [Risk management], Finansy i statistika Publ., Moscow, 288 p.
12. Matveev, B. A. (2007), *Spektralnyi metod otsenki i prognozirovaniia statisticheskikh riskov* [Spectral method of statistical estimation and forecasting of risks], YUrGU Publ., Chelyabinsk, 85 p.
13. Matveev, B. A. (2007), *Teoreticheskie osnovy issledovaniia statisticheskikh riskov* [Theoretical foundations of statistical studies of risks], YUrGU Publ., Chelyabinsk, 248 p.
14. Matveev, B. A., Sosnenko, L. S. (2009), *Signal riska i ego kharakteristiki* [Risk signal and its characteristics], *Upravlenie riskom*, No. 1 (49), pp. 2-8.
15. Matveev, B. A. (2010), *Spektralnyi pokazatel ekonomicheskogo riska* [The spectral index of economic risk], available at : <http://dspace.susu.ac.ru/handle/0001.74/1419> (accessed 12 September 2015).
16. Matveev, B. A. (2011), *Prognozirovanie ekonomicheskogo rezultata i svyazannogo s nim riska* [Predicting of the economic result and the related risk], *Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta*, No. 21 (238), pp. 54-58.
17. Matveev, B. A. (2012), *Spektralnyi podkhod k analizu i izmereniiu riska* [Spectral approach to the analysis and risk measurement], *Problemy analiza riska*, Vol. 9, No. 2, pp. 68-75.
18. Sosnenko, L. S., Matveev, B. A. (2013), *Spektralnyi pokazatel kachestva ekonomicheskoi modeli* [Spectral Quality of the economic model], *Vestnik Cheliabinskogo gosudarstvennogo universiteta*, No. 32 (323), *Ekonomika*, Iss. 42, pp. 5-9.
19. Matveev, B. A. (2014), *Spektralnaia teoriia riskov* [Spectral Risk Theory], *Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta*, Vol. 8, No. 2, pp. 20-24.
20. Matveev, B. A. (2015), *Osnovy spektralnoi teorii riskov* [Fundamentals of the spectral risks theory], *Upravlenie riskom*, No. 2, pp. 3-6.

21. Mokhor, V. V., Maksymenko, Y. V., Zinchenko, Y. V., Tsurkan, V. V. (2015), *Otsiniuvannia ryzyku bezpeky informatsii na osnovi spektralnoho pidkhodu* [Information security risk assessment based on spectral approach], XVII mizhnarodna naukovo-praktychna konferentsiia «Bezpeka informatsii v informatsiino-telekomunikatsiinykh systemakh», Kyiv, pp. 70.

22. Mokhor, V. V., Maksymenko, Y. V., Zinchenko, Y. V., Tsurkan, V. V. (2015), *Umovy vykorystannia spektralnoho pidkhodu dlia otsiniuvannia ryzyku bezpeky informatsii* [Terms of spectral approach to information security risk assessment], 7 vseukrainska naukovo-praktychna konferentsiia «Stan ta udoskonalennia bezpeky informatsiino-telekomunikatsiinykh system», Mykolaiv-Koblevo, pp. 72.

ЄВГЕНІЙ МАКСИМЕНКО,
ВАСИЛІЙ ЦУРКАН,
ЯРОСЛАВ ДОРОГОЙ,
ОЛЬГА КРУК

ОЦЕНИВАНИЕ РИСКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СПЕКТРАЛЬНОГО ПОДХОДА

Рассматривается использование систем управления безопасностью информации по результатам оценивания риска. Для этого через запланированные промежутки времени накапливаются статистические данные о угрозах и убытках вследствие их реализации. Как следствие, создаются предпосылки для использования статистического подхода. Однако, этот подход к оцениванию риска ограничивается высокими требованиями к объему статистических данных, завышением оценок риска, сложностью учета колебаний величины убытка, отсутствием единого эталона при сравнении рисков. Для преодоления обозначенных ограничений предлагается спектральный подход к оцениванию риска в системах управления безопасностью информации. Определяются условия его применения, в частности: накопление статистических данных о угрозах и убытках вследствие их реализации, учет динамики риска, установление эталона для сравнения рисков.

Ключевые слова: безопасность информации, риск, сигнал риска безопасности информации, оценивание риска, спектральный подход, система управления безопасностью информации.

YEVHEN MAKSYMENKO,
VASYL TSURKAN,
YAROSLAV DOROHYI,
OLHA KRUK

INFORMATION SECURITY RISK ASSESSMENT BASED ON SPECTRAL APPROACH

Using information safety managing systems on the results of the risk assessment is considering. Threats and damages statistics is collecting as a result of their implementation through the planned intervals. As a result, preconditions for using the statistical approach are created. However, the approach to risk assessment is limited by high requirements to the amount of statistics, overstated risk assessment, complexity of loss amount variation consideration, lack of a single standard when comparing risks. The risk assessment spectral approach for information safety managing systems is recommended to overcome the aforementioned limitations. Conditions of using the approach are analyzed, including: accumulating of statistics about the risks and losses due to their implementation, taking into account the risk dynamics, setting of standard for risks comparison.

Keywords: information security, risk, signal information security risk, risk assessment, spectral approach, information security management system.

Євген Васильович Максименко, заступник завідувача кафедри, Державний заклад «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

E-mail: iszzi@i.ua.

Василь Васильович Цуркан, кандидат технічних наук, провідний науковий співробітник, Державний заклад «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

E-mail: v.v.tsurkan@gmail.com.

Ярослав Юрійович Дорогий, кандидат технічних наук, доцент кафедри, Державний заклад «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

E-mail: argusyk@gmail.com.

Ольга Миколаївна Крук, молодший науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

E-mail: onk@conferen.ru

Евгений Васильевич Максименко, заместитель заведующего кафедрой, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, ведущий научный сотрудник, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Ярослав Юрьевич Дорогой, кандидат технических наук, доцент кафедры, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Ольга Николаевна Крук, младший научный сотрудник, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Yevhen Maksymenko, deputy head of academic department, State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, leading researcher, State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

Yaroslav Dorohyi, candidate of technical sciences, associate professor of academic department, State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

Olha Kruk, junior researcher, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.