INFORMATION SECURITY RISK MANAGEMENT

УДК 004.056.53

ВОЛОДИМИР МОХОР,
ВАСИЛЬ ЦУРКАН,
ЯРОСЛАВ ДОРОГИЙ,
СЕРГІЙ МИХАЙЛОВ,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ГЕОРГІЙ КРИХОВЕЦЬКИЙ,
ІГОР БОГДАНОВ

ВИКОРИСТАННЯ ЕНТРОПІЙНОГО ПІДХОДУ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

Розглядається ризик безпеки інформації як вплив невизначеності на досягнення цілей. Під досягненням цілей розуміється забезпечення конфіденційності, цілісності та доступності інформації. Оцінювання такого впливу здійснюється завдяки обиранню ентропії як міри невизначеності. Стан невизначеності описується кінцевою схемою. Для її визначення задаються множини загроз безпеці інформації та збитки внаслідок їх реалізації. При цьому враховується існування відмінних між собою загроз, що призводять до однакових збитків, а також загроз, унаслідок реалізації яких збитки відсутні. Водночас вважається відомим розподіл імовірностей нанесення збитків унаслідок реалізації загроз безпеці інформації. Коректність означеного підходу підтверджується виконанням властивостей ентропії. Тому використання ентропійного підходу дозволяє побудувати інтуїтивно більш коректну базу кількісного оцінювання ризиків безпеки інформації. Це обумовлено оперуванням формою розподілу випадкової величини, а не її конкретними значеннями. При цьому встановлюються переваги та недоліки ентропійного підходу. Для подолання означених недоліків у перспективах пропонується використання теорій нечітких множин і вірогідності.

Ключові слова: безпека інформації, ризик безпеки інформації, невизначеність, ентропія, ентропійний підхід.

Постановка проблеми. Нині ризик безпеки інформації тлумачиться як вплив невизначеності на досягнення цілей. Під досягненням цілей розуміється забезпечення конфіденційності, цілісності та доступності інформації. При цьому необхідно враховувати різноманітні фактори. З огляду на їх різноманіття варто зазначити, що невизначеності в цих факторах більше, ніж статистичної визначеності. Тому оцінювання невизначеності більш коректне на відміну від імовірності реалізації загрози безпеці інформації. Оскільки мірою невизначеності є ентропія, то пропонується використання ентропійного підходу для оцінювання ризиків безпеки інформації [1].

Аналіз останніх досліджень і публікацій. Ідея використання ентропії для оцінювання ризиків відома. Окремі її положення висловлювалися, наприклад, в [2-6]. Зокрема, досліджено ентропійні міри ризику при формуванні портфелю цінних паперів та експериментально встановлено значення параметра міри за якого досягається найкращий ефект [2]; описано методи визначення ентропії при оцінюванні ринкових ризиків [3]; розглянуто комбіновану ентропійну міру фінансових ризиків як випуклої комбінації ентропійної міри ризику та міри CVaR та проведено аналізування ефективності використання запропонованої міри [4]; розглянуто подолання проблеми формування портфелю заходів модернізації організацій для мінімізації господарських ризиків на основі їх інформаційно-ентпропійної моделі [5]; представлено систему підтримки прийняття рішень для керування портфелем цінних паперів на основі ентропійних мір ризику [6].

Однак, аналіз доступних джерел і матеріалів мережі Інтернет показав, що використання ентропійного підходу для визначення поняття "ризик безпеки інформації" вперше було запропоновано в [1] та розвинуто в [7].

Тому **метою статті є** проаналізувати використання ентропійного підходу для оцінювання ризиків безпеки інформації.

Виклад основного матеріалу дослідження [1, 7, 8]. Нехай для деякого об'єкту A апріорі відома множина з n загроз безпеці інформації і впорядкована множина з m станів збитку внаслідок реалізації цих загроз:

$$x_1, x_2, .., x_i, .., x_m,$$
$$i = \overline{1, m}.$$

Очевидно, що $n \le m$. Це вказує на існування не тотожних загроз безпеці інформації, які призводять до однакового збитку. Прикладом цьому можуть бути загрози внаслідок реалізації яких збитки рівні нулю.

Крім цього, під впорядкованістю розуміється, що

$$0 \le x_1 \le x_2 \le .. \le x_i \le .. \le x_m \le x_{\max},$$

де $x_{\max}$ – максимальний збиток, рівний повному ліквідуванню усіх інформаційних активів об'єкту A за нескінченно малий проміжок часу без будь-яких залишків. Крім цього вважатимемо, що відомий розподіл імовірностей p_i на множині x_i, а саме: збиток x_1 виникає з імовірністю p_1, збиток x_2 – з імовірністю p_2, збиток x_i – з імовірністю p_i.

З огляду на це, повною множиною подій $x_1, x_2, .., x_i, .., x_m$ назвемо таку множину станів збитку, що внаслідок реалізації загрози безпеці інформації обов'язково наступить один з них. Оскільки стани збитку $x_1, x_2, .., x_i, .., x_m$ повної множини подій задані з їх імовірностями

$$p_1, p_2, .., p_i, .., p_m,$$
$$p_i \ge 0, \sum_{i=1}^{m} p_i = 1,$$

то вважатимо заданою кінцеву схему

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_i & \dots & x_m \\ p_1 & p_2 & \dots & p_i & \dots & p_m \end{pmatrix}.$$

За допомогою кінцевої схеми описуватимемо стан невизначеності при забезпеченні конфіденційності, цілісності та доступності інформації. При цьому ступінь цієї невизначеності різна для різних схем. Тому для оцінювання ступеня невизначеності заданої кінцевої схеми використовується ентропійна міра

$$H_A(p_1, p_2, .., p_i, .., p_m) = -\sum_{i=1}^{m} p_i \lg p_i,$$

де $H_A(p_1, p_2, .., p_i, .., p_m)$ – ентропія кінцевої схеми (див. рис. 1), яку пропонується використовувати для оцінювання ризику безпеки інформації об'єкту A [8]. Якщо одне зі значень імовірності дорівнює одиниці, то функція $H_A(p_1, p_2, .., p_i, .., p_m) = 0$. Цьому відповідає випадок, коли завчасно можна передбачити реалізацію загрози безпеці інформації з повною достовірністю і, як наслідок, відсутністю невизначеності. Тоді як при фіксованому m найбільша невизначеність описуватиметься кінцевою схемою з рівноймовірними реалізаціями загроз.

Крім цього, коректність використання ентропійного підходу для оцінювання ризику безпеки інформації підтверджується такими властивостями ентропії [9]:

1. Величина

$$H_A(p_1, p_2, .., p_i, .., p_m) \ge 0.$$

Це означає, що ризик безпеки інформації може або дорівнювати нулю, або бути більшим за нього та, як наслідок, не може бути від'ємним. Цим пояснюється відмінність

ризиків безпеки від комерційних ризиків, де може існувати від'ємний ризик, що еквівалентний доходу на противагу збиткам при позитивному ризику.

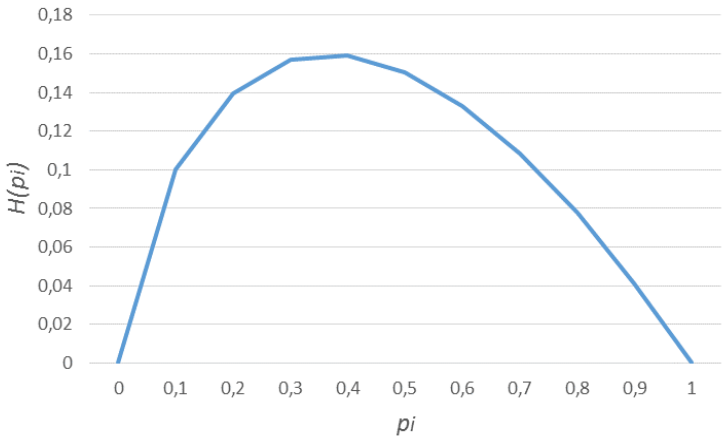

Рисунок 1 – Графічне відображення залежності ентропії кінцевої схеми

2. Якщо кінцеві схеми двох об'єктів A і B

$$X_1 = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1i} & \dots & x_{1m} \\ p_{11} & p_{12} & \dots & p_{1i} & \dots & p_{1m} \end{pmatrix}, \; X_2 = \begin{pmatrix} x_{21} & x_{22} & \dots & x_{2j} & \dots & x_{2n} \\ p_{21} & p_{22} & \dots & p_{2i} & \dots & p_{2n} \end{pmatrix}$$

взаємно незалежні, то

$$H_{AB}(X_1X_2) = H_A(X_1) + H_B(X_2).$$

Як наслідок, ризик безпеки інформації двох об'єктів A і B дорівнює сумі ризиків кожного з об'єктів. Це узгоджується з інтуїтивним уявленням про ризик безпеки інформації.

3. Якщо кінцеві схеми двох об'єктів A і B

$$X_1 = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1i} & \dots & x_{1m} \\ p_{11} & p_{12} & \dots & p_{1i} & \dots & p_{1m} \end{pmatrix}, \; X_2 = \begin{pmatrix} x_{21} & x_{22} & \dots & x_{2j} & \dots & x_{2n} \\ p_{21} & p_{22} & \dots & p_{2i} & \dots & p_{2n} \end{pmatrix}$$

взаємно залежні, то

$$H_{AB}(X_1X_2) = H_A(X_1) + H_B^{X_1}(X_2).$$

Як наслідок, ризик безпеки інформації об'єкту B зменшується якщо відомий результат реалізації загрози кінцевої схеми об'єкту A.

4. Якщо два об'єкта A і B мають однакові розподіли ймовірностей нанесення збитку внаслідок реалізації загроз, то ризик безпеки інформації для таких об'єктів однаковий.

5. Якщо

$$p_1 = p_2 = \dots = p_i = \dots = p_m = \frac{1}{m},$$

то величина $H_A(p_1, p_2, .., p_i, .., p_m)$ набуває найбільшого значення. Інтерпретація цієї властивості така: якщо для даного об'єкту нічого не відомо про ймовірності реалізації загроз, то ризик безпеки інформації максимальний. Використання засобів і заходів його оброблення по будь якій загрозі зменшує імовірність нанесення збитку при відповідному збільшенні ймовірності нульового збитку. Як наслідок, величина $H_A(p_1, p_2, .., p_i, .., p_m)$ буде зменшуватися, що свідчить про зменшення ризику безпеки інформації.

6. Для двох об'єктів A і B безпека інформації вища у того об'єкта, ризик безпеки інформації якого менший. Якщо $H_A(X_1) > H_B(X_2)$, то різниця $[H(A) - H(B)]$ показує, наскільки система керування безпекою інформації об'єкта B краща, ніж об'єкта A.

7. Якщо кінцева схема об'єкта A доповнюється неможливою подією

$$H_A(p_1, p_2, .., p_i, .., p_m, 0) = H_A(p_1, p_2, .., p_i, .., p_m),$$

то ентропія і, як наслідок, ризик безпеки інформації не змінюються.

Висновки. Використання ентропійного підходу дає можливість побудувати більш коректну базу кількісного оцінювання ризиків безпеки інформації. Це обумовлено оперуванням формою розподілу нанесення збитку, а не його конкретними значеннями. З іншого боку, ця перевага водночас є і недоліком. Оскільки виникає потреба у встановленні форми розподілу ймовірностей нанесення втрат унаслідок реалізацій загроз безпеці інформації.

Крім цього, необхідно сформувати повну множину реалізацій загроз, що ускладнюється відсутністю на практиці статистики збитків. Оскільки будь-який негативний прояв ризику в сфері безпеки повинен бути негайно оброблений з метою унеможливлювання його повторення в майбутньому, що призводить до невиконання умов стаціонарності спостережень.

У **перспективах подальших досліджень** планується використати теорії нечітких множин і вірогідності для подолання недоліків ентропійного підходу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В.В. Мохор, та В.В. Цуркан, “Энтропийный подход к определению понятия «риск информационной безопасности» (information security risk)”, на *XXVIII наук.-техн. конф. Моделювання*, Київ, 2009, с. 22.

[2] Е.М. Бронштейн, и О.В. Кондратьева, “Об эффективности использования энтропийных мер риска при формировании портфеля ценных бумаг”, *Финансовая аналитика: проблемы и решения*, т. 4, вып. 11, с. 7-10, март 2011.

[3] Р.А. Геворгян, “Энтропийный подход к оценке рыночных рисков”, *Управление финансовыми рисками*, № 2, с. 146-153, 2012.

[4] Е.М. Бронштейн, и О.В. Кондратьева, “Управление портфелем ценных бумаг на основе комбинированных энтропийных мер риска”, *Теория и системы управления*, № 5, с. 172, 2013.
doi: 10.7868/S0002338813050041

[5] Е.В. Левнер, и А.С. Птускин, “О выборе направлений модернизации предприятий на основе информационно-энтропийной модели хозяйственного риска”, *Экономика и математические методы*, т. 50, № 2, с. 111-126, 2014.

[6] Р.С. Ариаутов, А.Г. Пимонов, и К.Э. Рейзенбук, “Система поддержки принятия решений для управления портфелем ценных бумаг на основе энтропийных мер риска”, *Вестник Кузбасского государственного технического университета*, № 6, с. 169-174, 2015.

[7] В.В. Мохор, В.В. Цуркан, та С.М. Михайлов, “Ентропійний підхід до оцінювання ризику безпеки інформації в кіберпросторі”, на *IV міжн. наук.-практ. конф. ITSEC*, Київ, 2014, с. 43.

[8] А.Я. Хинчин, “Понятие энтропии в теории вероятностей”, *Успехи математических наук*, т. VIII, вып. 3 (55), с. 3-20, май-июнь 1953.

[9] М.В. Волькштейн, *Энтропия и информация*, Москва, Россия: Наука. 1986.

Стаття надійшла до редакції 20.09.2016.

REFERENCE

[1] V.V. Mokhor, and V.V. Tsurkan, “ The entropy approach to the definition of the "information security risk”, in Proc. *XXVIII conf. Modeling*, Kyiv, 2009, p. 22.

[2] E.M. Bronshtein, and O.V. Kondrateva, “ About efficiency of use entropic risk measures at securities portfolio forming”, *Financial Analytics: Science and Experience*, vol. 4, iss. 11, pp. 7-10, March 2011.

[3] R.A. Gevorgian, “Entropy approach to the market risks assessment”, *Financial Risk Management*, no. 2, pp. 146-153, 2012.

[4] E.M. Bronshtein, and O.V. Kondrateva, “Security portfolio management based on combined entropic risk measures”, *Theory and control systems*, no. 5, p. 172, 2013.
doi: 10.7868/S0002338813050041.

[5] E.V. Levner, and A.S. Ptuskin, “On the choice of directions of modernization of enterprises based on information entropy economic risk model”, *Economics and Mathematical Methods*, vol. 50, no. 2, pp. 111-126, 2014.
[6] R.S. Ariautov, A.G. Pimonov, and K.E. Reizenbuk, “Decision support system for securities portfolio management based on entropic risk measures”, *Vestnik of Kuzbass State Technical University*, no. 6, pp. 169-174, 2015.
[7] V.V. Mokhor, V.V. Tsurkan, and S.M. Mykhailov, “Entropy approach to information security risk assessment in cyberspace”, in *Proc. IV international conf. ITSEC*, Kyiv, 2014, c. 43.
[8] A.I. Khinchin, “The concept of entropy in probability theory”, *Uspekhi Matematicheskikh Nauk*, vol. VIII, iss. 3 (55), pp. 3-20, May-June 1953.
[9] M.V. Volkshtein, *Entropy and information.* Moscow, Russia: Nauka. 1986.

ВЛАДИМИР МОХОР,
ВАСИЛИЙ ЦУРКАН,
ЯРОСЛАВ ДОРОГОЙ,
СЕРГЕЙ МИХАЙЛОВ,
АЛЕКСАНДР БАКАЛИНСКИЙ,
ГЕОРГИЙ КРИХОВЕЦКИЙ,
ИГОРЬ БОГДАНОВ

ИСПОЛЬЗОВАНИЕ ЭНТРОПИЙНОГ ПОДХОДА ДЛЯ ОЦЕНИВАНИЯ РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Рассматривается риск безопасности информации как влияние неопределенности на достижение целей. Под достижением целей понимается обеспечение конфиденциальности, целостности и доступности информации. Оценивание такого влияния осуществляется благодаря выбору энтропии в качестве меры неопределенности. Состояние неопределённости описывается конечной схемой. Для ее определения задаются множества угроз безопасности информации и ущерба вследствие их реализации. При этом учитывается существование отличных между собой угроз, которые приводят к одинаковому ущербу, а также угроз, вследствие реализации которых отсутствует ущерб. Тем не менее считается известным распределение вероятностей нанесения ущерба вследствие реализации угроз безопасности информации. Корректность данного подхода подтверждается выполнением свойств энтропии. Поэтому использование энтропийного подхода позволяет построить интуитивно более корректную базу количественного оценивания рисков безопасности информации. Это обусловлено тем, что оперируют формой распределения случайной величины, а не ее конкретными значениями. При этом устанавливаются преимущества и недостатки энтропийного подхода. Для преодоления установленных недостатков в перспективе предлагается использование теорий нечетких множеств и возможности.

Ключевые слова: безопасность информации, риск безопасности информации, неопределенность, энтропия, энтропийный подход.

VOLODYMYR MOKHOR,
VASYL TSURKAN,
YAROSLAV DOROHYI,
SERHII MYKHAILOV,
OLEKSANDR BAKALYNSKYI,
HEORHII KRYKHOVETSKYI,
IHOR BOHDANOV

USE OF ENTROPYNY APPROACH FOR INFORMATION SECURITY RISKS ASSESSMENT

The risk of information security as an influence of uncertainty on the achievement of goals is considered. In achieving the goals meant to ensure the confidentiality, integrity and availability of

information. Estimation of such influence is carried out by the elimination of entropy as a measure of uncertainty. The state of uncertainty is described by the final scheme. The variety of threats for information security and loss resulting from their implementation is set for its definition. It takes into account the existence of different threats that lead to the same losses, and threats, due to the implementation of which there are no losses. At the same time, the distribution of likelihood of damage as a result of the implementation of threats for information security is considered as known. The correctness of that approach is confirmed by the implementation of the entropy characteristics. Therefore, the use of an entropy approach allows to construct an intuitively more correct basis for quantitative risk assessment of information security. It is associated with a fact of operating the form of the distribution of a random variable but not its specific values. In this case, the advantages and disadvantages of the entropy approach are established. The using of fuzzy set theory and likelihood is offered to overcome the identified shortcomings in prospect.

Keywords: information security, information security risk, uncertainty, entropy, entropy approach.

Володимир Володимирович Мохор, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

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

Василь Васильович Цуркан, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

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

Ярослав Юрійович Дорогий, кандидат технічних наук, доцент, докторант, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: argusyk@gmail.com.

Сергій Миколайович Михайлов, здобувач, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: mixserg@bk.ru.

Олександр Олегович Бакалинський, заступник завідувача кафедри управління та тактико-спеціальної підготовки, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: baov@meta.ua.

Георгій Яремович Криховецький, кандидат технічних наук, старший науковий співробітник, начальник науково-організаційного відділу, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: kgeorg@ukr.net.

Ігор Олександрович Богданов, молодший фахівець, "Старком" ДП "ССМ", Київ, Україна.

E-mail: Bogdanovigr@gmail.com.

Владимир Владимирович Мохор, доктор технических наук, профессор, директор, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Ярослав Юрьевич Дорогой, кандидат технических наук, доцент, докторант, Национальный технический университет Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Сергей Николаевич Михайлов, соискатель, Институт специальной связи и защиты информации Национального технического университета Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Александр Олегович Бакалинський, заместитель заведующего кафедрой управления и тактико-специальной подготовки, Институт специальной связи и защиты информации Национального технического университета Украины ”Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Георгий Яремович Криховецкий, кандидат технических наук, старший научный сотрудник, начальник научно-организационного отдела, Институт специальной связи и защиты информации Национального технического университета Украины ”Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Игорь Александрович Богданов, младший специалист, “Старком” ДП “ССМ”, Киев, Украина.

Volodymyr Mokhor, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communications and information protection National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Yaroslav Dorohyi, candidate of technical sciences, associate professor, doctoral student, National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Serhii Mykhailov, postgraduate student, Institute of special communications and information protection National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Oleksandr Bakalynskyi, deputy head of management and tactical and special training academic department, Institute of special communications and information protection National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Heorhii Krykhovetskyi, candidate of technical sciences, senior researcher, chief of the scientific-organizational department, Institute of special communications and information protection National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Ihor Bohdanov, junior, “Starcom” “CCM” Subsidiary Enterprise, Kyiv, Ukraine.