**УДК 004.051:004.056.5**

**М. А. Стрельбіцький**

# ФОРМУВАННЯ МНОЖИНИ ДОПУСТИМИХ ЗНАЧЕНЬ ПОКАЗНИКА ЯКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

*У статті проведено аналіз існуючих підходів до оцінювання ефективності системи захисту інформації. Отримано функціональні залежності закону розподілу випадкового вектора вершини множини допустимих значень показника якості системи захисту інформації з урахуванням умовних ймовірностей порушення властивостей інформації.*

*К л ю ч о в і  с л о в а :  захист інформації, множина загроз, інформаційно-телекомунікаційна система.*

**Постановка проблеми.** Значні масштаби інформатизації та широке впровадження у сферу обробки інформації автоматизованих систем на базі програмно-апаратних комплексів дозволили розгорнути та більше 10 років експлуатувати інтегровану інформаційно-телекомунікаційну систему прикордонного відомства "Гарт", призначену для створення єдиного інформаційного простору суб'єктів інтегрованого управління кордонами та електронної системи управління Державної прикордонної служби України, виконання завдань з підвищення ефективності управління органами зазначеної служби під час охорони державного кордону.

Державна прикордонна служба України як суб'єкт забезпечення національної безпеки у своїй діяльності використовує прикордонний інформаційний ресурс, який є складовою інформаційного ресурсу держави [1] та потребує захисту. Відповідно до закону [2] захист інформації в інформаційно-телекомунікаційній системі (ІТС) – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Таке визначення дозволяє сформулювати поняття захисту інформації як цілеспрямованого процесу з єдиною (що є принциповим) метою – недопущення несанкціонованих дій стосовно інформації під час всього життєвого циклу системи "Гарт". Питання оптимізації цього складного організаційно-технологічного процесу є важливим завданням, що потребує визначення кількісних та якісних оцінок його ефективності.

**Аналіз останніх досліджень і публікацій.** Вирішенню завдання створення, організації, дослідження ефективності функціонування систем захисту інформації (СЗІ) присвячені праці вчених В. Б. Дудикевича, В. А. Герасименка, О. Г. Корченка, Г. Ф. Конаховича, В. А. Хорошка та багатьох інших, у яких застосовано широкий спектр підходів до оцінювання ефективності СЗІ, основними з них є:

– вартісний підхід – підхід з погляду на цінність інформації (втрати цінності інформації у разі порушення її властивостей, загальні збитки при втраті інформації, вартість організаційно-технічних заходів, які застосовуються в СЗІ, тощо);

– оцінювання якості СЗІ за заданими показниками та обмеженнями системи;

– інтегральне оцінювання (згортання часткових показників якості, методи теорії нечітких множин, нейронних мереж, графів тощо);

– ймовірнісний підхід – розгляд СЗІ з погляду на ступінь придатності системи до виконання завдань в конкретних умовах функціонування.

Проте при застосуванні ймовірнісного підходу в теорії ефективності складних систем сьогодні недостатньо повно розглянуто спосіб формування множини допустимих значень показника якості СЗІ.

**Мета статті.** На підставі аналізу загроз інформації визначити функції розподілу компонент вектора допустимих значень показника якості СЗІ.

**Виклад основного матеріалу.** Для оцінювання ефективності функціонування СЗІ необхідно розробити показник ефективності процесу захисту інформації, який повинен відповідати таким основним вимогам [3]: показовість (адекватність), критичність (чутливість), комплексність (повнота), стохастичність, простота.

Поняття "захист інформації" можна розглядати як сукупність (послідовність) узгоджених дій протягом певного часу, спрямованих на досягнення мети цього процесу. Оцінюючи ефективність, необхідно звернути увагу на те, що це властивість процесу, а не самої системи. Тому в подальшому під поняттям ефективності захисту інформації будемо розуміти комплексну властивість цілеспрямованого процесу, який характеризується ступенем досягнення мети, а саме – захист інформації.

Оцінюючи якість СЗІ, яка описується $n$-вимірним векторним показником $Y_{\langle n\rangle}$, необхідно визначити сукупність критеріїв, що належать класу критеріїв придатності $\{G\}$. Математичне формулювання останнього має такий вигляд [3]:

$$G:\left(Y_{\langle n\rangle}\in\left\{Y^{A}_{\langle n\rangle}\right\}\right), \tag{1}$$

де $Y_{\langle n\rangle}$ – показник якості СЗІ; $\left\{Y^{A}_{\langle n\rangle}\right\}$ – множина допустимих значень (**A**llow values) показника якості СЗІ.

Таким чином, СЗІ, для якої справедлива умова (1), придатна до використання за призначенням та виконує свої функції.

У нормативному документі [4] визначені функціональні критерії, які описують вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: конфіденційності, цілісності, доступності, спостереженості, що визначає множину типів показників якості СЗІ (властивостей інформації):

$$\Re=\{i,c,a,u\}, \tag{2}$$

де $i$ – цілісність (**i**ntegrity); $c$ – конфіденційність (**c**onfidentiality); $a$ – доступність (**a**vailability); $u$ – спостереженість (acco**u**ntability).

Враховуючи вираз (2), кожна з компонент вектора допустимих значень

$$Y^{A}=\left\langle v^{A}_{i},v^{A}_{c},v^{A}_{a},v^{A}_{u}\right\rangle,$$

де $v^{A}_{i}$ – показник цілісності; $v^{A}_{c}$ – показник конфіденційності; $v^{A}_{a}$ – показник доступності; $v^{A}_{u}$ – показник спостереженості, залежить від умов застосування системи і визначається управляючою системою

$$Y^{A}=Y^{A}\left(B\right), \tag{3}$$

де $B$ – характеристики умов застосування СЗІ.

Семантикою показників якості системи захисту інформації є значення часу, протягом якого властивість інформації не буде порушена.

У загальному випадку на характеристики СЗІ, її організацію, умови функціонування та застосування діє множина випадкових факторів, що визначає зазначені величини як випадкові. Разом із тим апріорі випадковими є і допустимі значення вектора $Y^{A}$, який залежить від умов застосування системи, так як завчасно невідомо, які повинні бути результати роботи СЗІ, щоб забезпечити необхідний рівень захисту.

Таким чином, всі складові вектора допустимих значень показників якості функціонування СЗІ мають ймовірнісний характер, тому:

$$\hat{Y}^{A}=Y^{A}\left(\hat{B}\right). \tag{4}$$

Зауважимо, що однобічність вимог до характеристик СЗІ є принциповою. Це дозволяє описати множину допустимих значень показника якості придатності СЗІ чотиривимірним гіпероктантом

$$\left\{\hat{Y}^{A}\right\}=\left(\hat{v}_{i}^{A},\infty\right)\times\left(\hat{v}_{c}^{A},\infty\right)\times\left(\hat{v}_{a}^{A},\infty\right)\times\left(\hat{v}_{u}^{A},\infty\right) \quad (5)$$

з вершиною в точці $\hat{Z}=\left\langle\hat{v}_{i}^{A},\hat{v}_{c}^{A},\hat{v}_{a}^{A},\hat{v}_{u}^{A}\right\rangle$.

Отже, опис множини допустимих значень показника якості придатності СЗІ зводиться до відшукання законів розподілу компонент вектора $\hat{Z}$.

Відповідно до нормативного документа [5] за результатами обстеження середовищ функціонування ІТС визначаються потенційні загрози для інформації і розробляється модель загроз. Побудова моделі здійснюється згідно з положеннями нормативних документів [6–8]. Після побудови комплексної СЗІ сформуємо уточнену множину загроз $\{T\}$ складовим інформації в ІТС, на підставі яких формуються компоненти вектора допустимих значень $Y^{A}$.

Нехай $P_{p}^{A}$ – ймовірність порушення p-ї $(p\in\Re)$ властивості інформації, яка залежить від імовірності реалізації загрози

$$P_{p}^{A}\left(v_{p}^{A}\right)=1\text{-}P\left(\hat{v}_{p}^{A}\le v_{p}^{A}\right). \quad (6)$$

Множину загроз $\{T\}$ розділимо за загрозами щодо кожної властивості інформації p – $\left\{T^{p}\right\}$. Кожну із цих підмножин також розділимо на дві підмножини: $\left\{T_{ind}^{p}\right\}$ – група загроз, імовірність виникнення яких не залежить від модернізації ІТС, та $\left\{T_{dep}^{p}\right\}$ – група загроз, імовірність виникнення яких залежить від модернізації ІТС за умови

$$\begin{gathered}\left\{T_{dep}^{p}\right\}\cup\left\{T_{ind}^{p}\right\}=\left\{T^{p}\right\},\\ \left\{T_{dep}^{p}\right\}\cap\left\{T_{ind}^{p}\right\}=\varnothing\end{gathered} \quad (7)$$

.

Таким чином, імовірність порушення властивості інформації становить

$$P_{p}^{A}\left(v_{p}^{A}\right)=1-\prod_{\forall k\in\left\{T_{ind}^{p}\right\}}\left(1-P_{p,k}^{ind}\right)\prod_{\forall k\in\left\{T_{dep}^{p}\right\}}\left(1-P_{p,k}^{dep}\left(\hat{v}_{p}^{A}\le v_{p}^{A}\right)\right), \quad (8)$$

де $P_{p,k}^{ind}$ – ймовірність порушення p-ї властивості інформації при реалізації k-ї загрози; $P_{p,k}^{dep}(t)$ – ймовірність порушення p-ї властивості інформації при реалізації k-ї загрози у разі модернізації ІТС протягом часу $v_{p}^{A}$.

Визначимо ймовірність порушення p-ї властивості інформації при реалізації k-ї загрози, яка не залежить від модернізації ІТС та може бути описана законом розподілу

$$F_{p,k}^{ind}(t)=\begin{cases}0, t<0\\ P_{p,k}^{ind}\\ 1, t>t_{експл}\end{cases}, \quad (9)$$

де $t_{експл}$ – час експлуатації СЗІ.

Визначимо ймовірність порушення безпеки інформації, яка залежить від модернізації ІТС, тобто від потоку дестабілізуючих факторів на етапі припрацювання модернізованої складової.

Очевидно, що в загальному випадку найбільш повно описує ймовірність виникнення загрози функція розподілу цієї випадкової величини. Разом із тим при конкретному формуванні множини загроз та визначенні експертами самого факту функціональної залежності загрози від модернізації формування виду та параметрів функції розподілу є малоймовірним. Тому пропонується як оцінку значення цієї ймовірності використовувати експертне значення величини ймовірності виникнення загрози з урахуванням ймовірності виникнення дестабілізуючого фактора, яка описується розподілом Вейбула, що своєю чергою описує час безвідмовної роботи та застосовується для оцінювання надійності програмних засобів [9].

Таким чином, імовірність виникнення загрози інформації, яка залежить від модернізації ІТС, становить:

$$P_{p,k}^{dep}(\hat{v}_p^A \le v_p^A)=F_{p,k}^{dep}(v_p^A)=1-e^{-\left(\frac{v_p^A}{\beta_{p,k}}\right)^{\alpha_{p,k}}}. \quad (10)$$

На практиці аналітичне визначення параметрів розподілу Вейбула за статистичними даними достатньо складне. Використовуючи наближений метод та дані випробувань, можливо визначити значення параметрів $\alpha_{p,k}$ та $\beta_{p,k}$ [10]. Отже, вираз (8) набиратиме такого вигляду:

$$P_p^A\left(v_p^A\right)=1-\prod_{\forall k\in\left\{T_{ind}^p\right\}}\left(1-F_{p,k}^{ind}\left(v_p^A\right)\right)\prod_{\forall k\in\left\{T_{dep}^p\right\}}e^{-\left(\frac{v_p^A}{\beta_{p,k}}\right)^{\alpha_{p,k}}}. \quad (11)$$

Отримані функціональні залежності дозволяють сформувати закон розподілу випадкового вектора $\hat{Z}$:

$$F_{\hat{Z}}\left(Y^A\right)=P\left[\left(\hat{v}_i^A\le v_i^A\right)\cap\left(\hat{v}_c^A\le v_c^A\right)\cap\left(\hat{v}_a^A\le v_a^A\right)\cap\left(\hat{v}_u^A\le v_u^A\right)\right]. \quad (12)$$

У загальному випадку події, пов'язані з порушенням властивостей інформації, є взаємозалежними. Тому для формування закону розподілу випадкового вектора $\hat{Z}$ не достатньо знати закони розподілу кожної із випадкових величин, а потрібно ще знати закони зв'язку між ними. Цей зв'язок характеризують за допомогою умовних законів розподілу. Маючи вид та характеристики умовних законів розподілу, не важко сформувати загальну функціональну залежність (12).

Разом із тим отримання умовних законів розподілу при формуванні СЗІ є проблемним. З метою оцінювання ступеня залежності показників якості системи захисту інформації пропонується використати метод експертних оцінок або статистичне значення ймовірностей виникнення події порушення властивості інформації за умови порушення іншої (якщо вона є).

Значення умовних імовірностей сформуємо у вигляді таблиці.

*Значення умовних ймовірностей порушення властивостей інформації*

| Властивість інформації | Умовна ймовірність порушення властивості інформації | | | |
|---|---|---|---|---|
| | цілісність | конфіденційність | доступність | спостереженість |
| цілісність | 1 | $P_i(c)$ | $P_i(a)$ | $P_i(u)$ |
| конфіденційність | $P_c(i)$ | 1 | $P_c(a)$ | $P_c(u)$ |
| доступність | $P_a(i)$ | $P_a(c)$ | 1 | $P_a(u)$ |
| спостереженість | $P_u(i)$ | $P_u(c)$ | $P_u(a)$ | 1 |

Визначимо множину гіпотез

$$H=\left\{H_i,H_c,H_a,H_u,H_d\right\}, \quad (13)$$

де $H_i$ – порушення цілісності інформації; $H_c$ – порушення конфіденційності інформації; $H_a$ – порушення доступності інформації; $H_u$ – порушення спостереженості інформації; $H_d$ – дотримання безпеки інформації.

Очевидно, що

$$\left(1-P\left(H_i\right)\right)\cdot\left(1-P\left(H_c\right)\right)\cdot\left(1-P\left(H_a\right)\right)\cdot\left(1-P\left(H_u\right)\right)+P\left(H_d\right)=1, \quad (14)$$

звідки

$$P\left(H_d\right)=1-\left(1-P\left(H_i\right)\right)\cdot\left(1-P\left(H_c\right)\right)\cdot\left(1-P\left(H_a\right)\right)\cdot\left(1-P\left(H_u\right)\right). \quad (15)$$

Визначимо аналітичні залежності для гіпотези $H_i$ за умови порушення тільки конфіденційності $P_c(i)$. Для цього сформуємо повну групу подій

$$\Omega=\left\{\omega_1,\omega_2,\omega_3\right\}, \quad (16)$$

де $\omega_1$ – порушення конфіденційності інформації, яке не призвело до порушення цілісності; $\omega_2$ – порушення конфіденційності інформації, яке призвело до порушення цілісності; $\omega_3$ – порушення конфіденційності інформації відсутнє.

Таким чином, порушення цілісності інформації за умови порушення конфіденційності становить

$$P_{H_1}^{c} = P_i(v_i^A) + \left(1 - P_i(v_i^A)\right) \times \left(1 - \left[\left(1 - P_c(v_i^A) + P_c(v_i^A)\left(1 - P_c(i)\right)\right)\right]\right). \quad (17)$$

Використовуючи цей підхід, поширимо множину подій на решту властивостей. Таким чином, порушення цілісності інформації є зворотна подія до події не порушення цілісності, з урахуванням імовірностей порушень інших властивостей:

$$\begin{aligned} P_{H_i}\left(v_i^A\right) &= P_i(v_i^A) + (1 - P_i(v_i^A)) \times \left(1 - \left[\left(1 - P_c(v_i^A)\right) + P_c(v_i^A)\left(1 - P_c(i)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_i^A)\right) + P_a(v_i^A)\left(1 - P_a(i)\right)\right]\right) \times \left(1 - \left[\left(1 - P_u(v_i^A)\right) + P_u(v_i^A)\left(1 - P_u(i)\right)\right]\right). \end{aligned} \quad (18)$$

Аналогічно для інших гіпотез:

$$\begin{aligned} P_{H_c}\left(v_c^A\right) &= P_c(v_c^A) + (1 - P_c(v_c^A)) \times \left(1 - \left[\left(1 - P_i(v_c^A)\right) + P_i(v_c^A)\left(1 - P_i(c)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_a(v_c^A)\right) + P_a(v_c^A)\left(1 - P_a(c)\right)\right]\right) \times \left(1 - \left[\left(1 - P_u(v_c^A)\right) + P_u(v_c^A)\left(1 - P_u(c)\right)\right]\right), \end{aligned} \quad (19)$$

$$\begin{aligned} P_{H_a}\left(v_a^A\right) &= P_a(v_a^A) + (1 - P_a(v_a^A)) \times \left(1 - \left[\left(1 - P_i(v_a^A)\right) + P_i(v_a^A)\left(1 - P_i(a)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_a^A)\right) + P_c(v_a^A)\left(1 - P_c(a)\right)\right]\right) \times \left(1 - \left[\left(1 - P_u(v_a^A)\right) + P_u(v_a^A)\left(1 - P_u(a)\right)\right]\right), \end{aligned} \quad (20)$$

$$\begin{aligned} P_{H_u}\left(v_u^A\right) &= P_u(v_u^A) + (1 - P_u(v_u^A)) \times \left(1 - \left[\left(1 - P_i(v_u^A)\right) + P_i(v_u^A)\left(1 - P_i(u)\right)\right]\right) \times \\ &\times \left(1 - \left[\left(1 - P_c(v_u^A)\right) + P_c(v_u^A)\left(1 - P_c(u)\right)\right]\right) \times \left(1 - \left[\left(1 - P_a(v_u^A)\right) + P_a(v_u^A)\left(1 - P_a(u)\right)\right]\right). \end{aligned} \quad (21)$$

Враховуючи формули (12, 18–21), отримаємо аналітичну форму закону розподілу випадкового вектора $\hat{Z}$:

$$F_{\hat{Z}}\left(Y^A\right) = \left(1 - P_{H_i}\left(v_i^A\right)\right) \times \left(1 - P_{Hc}\left(v_c^A\right)\right) \times \left(1 - P_{H_a}\left(v_a^A\right)\right) \times \left(1 - P_{H_u}\left(v_u^A\right)\right). \quad (22)$$

Таким чином, отримані функціональні залежності дозволяють описати множину допустимих значень показника якості системи захисту інформації.

## Висновки

Запропонований підхід до формування множини допустимих значень показника якості системи захисту інформації дозволить врахувати динамічний потік дестабілізуючих факторів, спричинених процесом модернізації складових ІТС при оцінюванні ефективності СЗІ в реальних умовах. У формуванні закону розподілу випадкового вектора вершини гіпероктанта допустимих значень враховані умовні ймовірності порушення властивостей інформації. В подальшому визначений закон розподілу доцільно використовувати у розробленні методу оцінювання ефективності функціонування системи захисту інформації ІТС.

## Список використаних джерел

1. Стрельбіцький, М. А. Прикордонний інформаційний ресурс: визначення поняття [Текст] / М. А. Стрельбіцький // Сучасні інформаційні технології у сфері безпеки та оборони. – 2016. – № 1 (25). – С. 205–208.

2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Текст] // Відомості Верховної Ради України (ВВР). – 1994. – № 31. – Ст. 286.

3. Петухов, Г. Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремлённых систем [Текст] / Г. Б. Петухов, В. И. Якунин. – М. : АСТ, 2006. – 504 с.

4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТ СЗІ СБ України від 28.04.1999 р. № 22. Із змінами згідно з наказом адміністрації Держспецзв'язку від 28.12.2012 р. № 806.

5. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТ СЗІ СБ України від 08.11.2005 р. № 125.

6. НД ТЗІ 1.1-002. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТ СЗІ СБ України від 28.04.1999 р. № 22.

7. НД ТЗІ 1.4-001. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТ СЗІ СБ України від 04.12.2000 р. № 53.

8. НД ТЗІ 1.6-003. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації. Затверджено наказом ДСТ СЗІ СБ України від 08.11.2005 р. № 125 із змінами згідно з наказом адміністрації Держспецзв'язку від 28.12.2012 р. № 806.

9. Усенко, О. А. Модели и методы оценки надежности программного обеспечения информационных систем [Текст] : учеб. пособие / О. А. Усенко. – Таганрог : ТТИ ЮФУ, 2008. – 40 с.

10. Овчинников, П. Ф. Высшая математика [Текст] : учеб. пособие / П. Ф. Овчинников, Б. М. Лисицын, В. М. Михайленко. – К. : Вища шк., 1989. – 679 с.

*Стаття надійшла до редакції 31.05.2017 р.*

**УДК 004.051:004.056.5**

**М. А. Стрельбицкий**

**ФОРМИРОВАНИЕ МНОЖЕСТВА ДОПУСТИМЫХ ЗНАЧЕНИЙ ПОКАЗАТЕЛЯ КАЧЕСТВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА СТАДИИ МОДЕРНИЗАЦИИ**

*В статье проведен анализ существующих подходов к оценке эффективности системы защиты информации. Получены функциональные зависимости закона распределения случайного вектора вершины множества допустимых значений показателя качества системы защиты информации с учетом условных вероятностей нарушения свойств информации.*

*К л ю ч е в ы е  с л о в а :  защита информации, множество угроз, информационно-телекоммуникационная система.*

**UDC 004.051:004.056.5**

**M. A. Strelbtskiy**

**FORMATION OF THE SET OF ACCEPTABLE VALUES OF THE INFORMATION SECURITY SYSTEM QUALITY INDICATOR AT THE STAGE OF INFORMATION AND TELECOMMUNICATION SYSTEM MODERNIZATION**

*The article analyzes the existing approaches to evaluating the effectiveness of the information security system. The resulting functional dependencies allowed to form a distribution law of random vector of peak set acceptable values of the information security system quality indicator considering the conditional probabilities of information property breach.*

*K e y w o r d s :  information security, set of threats, information and telecommunication system.*

**Стрельбіцький Михайло Анатолійович** – кандидат технічних наук, доцент, докторант Національної академії Державної прикордонної служби України імені Б. Хмельницького.