УДК 629.735 DOI: 10.30748/soivt.2018.56.13

Д.С. Комін[1], О.В. Чечуй[1], М.А. Левченко[2], О.С. Панхохін[1], В.А. Павловський[1]

[1]*Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*
[2]*Інститут авіації та протиповітряної оборони Національного університету оборони України ім. І. Черняховського, Київ*

ФОРМАЛІЗОВАНА МОДЕЛЬ ОЦІНКИ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуті особливості проведення оцінювання гарантій інформаційної безпеки для комплексної системи захисту інформації у відповідності до державних та міжнародних стандартів. Запропоновано застосування формалізованої моделі процесу оцінювання вимог гарантій інформаційної безпеки суб'єктів експертизи із застосуванням аксіоматичних конструкцій. Така модель дозволяє здійснювати дослідження процесу оцінювання гарантій інформаційної безпеки та визначати вимоги до результатів експертизи, щодо неупереджуваності, об'єктивності, повторюваності, відтворюваності і порівнянності.

Ключові слова: *комплексна система захисту інформації, інформаційно-телекомунікаційна система, інформаційна безпека, суб'єкт експертизи, об'єкт експертизи, формалізована модель, експерт.*

Вступ

Постановка проблеми. Невід'ємною частиною будь-якої інформаційно-телекомунікаційної системи (ІТС) військового призначення, особливо там, де здійснюється обробка інформації з обмеженим доступом (ІзОД), є комплекс заходів, пов'язаний із забезпеченням збереження, цілісності інформації та належного порядку доступу до неї. Для цього розробляється та впроваджується в ІТС комплексна система захисту інформації (КСЗІ). Для оцінки якості та відповідності КСЗІ проводиться експертиза із залученням відповідних організацій та компетентних експертів, які мають оцінити рівень гарантій інформаційної безпеки (ІБ). До процесу оцінювання висуваються вимоги широти, глибини та суворості, а до результатів оцінювання – вимоги об'єктивності, неупередженості, повторюваності, відтворюваності та співставленості. Однією з основних проблем, які виникають під час оцінки гарантій ІБ, є те, що для більшості вимог гарантій застосовуються лише якісні характеристики. Отже актуальним є завдання формалізації як безпосередньо процесу оцінювання гарантій, так і формалізації вимог до процесу та результатів оцінювання гарантій.

Аналіз останніх досліджень і публікацій. В [1–4] розглянуто різні методи представлення ІТС за допомогою яких вирішується задача оцінки гарантій ІБ у відповідності до вимог стандартів [5–7]. Огляд нормативної та наукової літератури показав, що на сьогодні шляхи (способи, методи) забезпечення виконання вимог до процесу та результатів оцінювання не визначені.

Це обумовлено: недостатньою глибиною вивчення природи даних вимог; відсутністю формального формулювання та представлення вимог; відсутністю формальної постановки завдань на забезпечення даних вимог; відсутністю формальних моделей проведення експертизи (оцінювання) та формального представлення результатів.

Мета статті. В даній статті пропонується застосування формалізованого підходу для побудови моделі оцінки гарантій ІБ КСЗІ з позиції процесного підходу та формального представлення вимог, які висуваються до результатів експертизи.

Виклад основного матеріалу

Оскільки оцінка гарантій ІБ є діяльністю, яка включає процеси взаємодії суб'єктів експертизи і процеси виконання дій з оцінки в ході експертизи, то до оцінки гарантій доцільно підходити з позицій процесного підходу. В [8] розглянуто загальні ознаки будь-якого процесу, а також проаналізовано різні визначення процесу. Завдяки ним надамо наступне визначення.

Процес оцінки вимог гарантій ІБ – це сукупність взаємопов'язаних операцій та дій, які направлені на дослідження, перевірку, аналіз та оцінку об'єкта експертизи, шляхом перетворення вхідних матеріальних та інформаційних потоків у вихідні потоки, які необхідні для суб'єктів експертизи, з метою визначення ступеня відповідності характеристик об'єкта експертизи заданим вимогам і визначення можливості використання об'єкта, який оцінюється, у якості довіреного з точки зору безпеки інформації.

При розробці моделі процесу оцінки гарантій ІБ були враховані наступні аспекти:

– функціональний, який точно визначає, що здійснюється елементами процесу;

– інформаційний, який відображає інформаційну сутність, що формується, виробляється або використовується процесом;

– організаційний, який описує хто і коли виконує конкретні дії, роботи, операції процесу із включенням фізичних механізмів передачі та зберігання об'єктів;

– каузальний, який відноситься до координації і залежності дій, суб'єктів цих дій.

В основі формалізованої моделі процесу оцінки вимог гарантій ІБ застосовані наступні аксіоматичні конструкції (АК):

АК 1. Процес оцінки гарантій складає набір (множину) дій $A = \{A_n \mid n = \overline{1, N}\}$ з оцінки вимог гарантій.

Дії описують роботи, які виконують експерти та інші учасники процесу оцінювання. У загальному випадку, сукупність дій може бути представлена у вигляді графа G^A, який описує конкретні типи відносин на множині дій. Множина дій складає методику оцінювання.

АК 2. Множина відношень $D = \{D_m \mid m = \overline{1, M}\}$ різного типу, які визначені на множині A.

Множина дій A створює процес $Z(A, d)$, якщо $A \in \overline{A}$ і на цій множині задано відношення $d(A) \in D$. Відношення d може бути, наприклад, відношенням типу "частина-ціле", "каузальна залежність" та ін. Універсальна множина дій з оцінки гарантій визначається у нормативних документах [9]. Для створення процесу на множині A необхідно як мінімум задати відношення залежності (домінування). У цьому випадку множина дій може розглядатися як послідовність дій.

АК 3. Призначення процесу формується метою TRG та результатами, які очікуються REZ:

$$\text{Purpose} =< TRG, REZ > . \qquad (1)$$

Процес реалізується і виконується для досягнення конкретної мети і отримання результатів, які потрібні для учасників процесу. Мета виступає системоутворюючим фактором і визначає відношення на множині дій. При визначенні гарантій ІБ головною метою постає встановлення ступеня задоволення множині вимог, які задані, та відповідності об'єкта експертизи визначеному рівню гарантій безпеки.

Головна мета може бути декомпозована на підцілі, а саме на сукупність властивостей $P = \{P_j \mid j = \overline{1, J}\}$, які повинен мати об'єкт експертизи для задоволення вимогам гарантій. Множина властивостей може бути представлена у вигляді графа $G^P = \{P, D\}$, де D – множина відношень, які встановлюються на множині властивостей.

Множина властивостей складає програму оцінювання PR.

У якості результату REZ процесу оцінювання виступає множина висновків (вердиктів) експертів $V = \{V_i \mid i = \overline{1, I}\}$ відносно ступеня прояву окремих властивостей гарантій безпеки. Ці вердикти оформлюються у вигляді звіту (експертного висновку), що є матеріальним виразом результату оцінювання гарантій безпеки.

Аналіз вимог гарантій, які закріплені нормативними документами [6–7], дозволяє зробити висновок, що вимоги у більшій ступені носять якісний характер, і кількісно не можуть бути визначені. Таке представлення ускладнює їх аналіз і одним з шляхів вирішення даної задачі є використання апарату лінгвістичних змінних, які дозволяють задавати формальне значення змінних у вигляді вербальних виразів. При використанні такого підходу для кожної властивості вводиться лінгвістична змінна L і визначається її терм-множина β_L, тобто множина значень, які вона може приймати. Таким чином, кожний вердикт є відображенням значення лінгвістичної змінної, яке вона прийняла в ході експертизи. Формально можна сказати, що кожний вердикт V_i містить значення лінгвістичної змінної i-ї властивості, а сам звіт можна представити у вигляді множини значень лінгвістичних змінних $V = \{L_i \mid i = \overline{1, I}\}$.

Таким чином, призначення процесу оцінювання гарантій безпеки буде формувати дерево цілей G^P, яке описується у програмі оцінювання і множина вердиктів V, які представлені у вигляді звіту:

$$\text{Purpose} =< G^P, V > . \qquad (2)$$

АК 4. Множина входів $IN = \{I^{in}, M^{in}\}$ і виходів $OUT = \{I^{out}, M^{out}\}$ процесу Z із заданим оператором перетворення $F : IN \to OUT$.

У загальному випадку входи і виходи процесу являють собою матеріальні та інформаційні потоки. Матеріальний потік M уявляє собою безперервну або дискретну множину матеріальних об'єктів $M = \{m_q \mid q = \overline{1, Q}\}$, які розподілені у часі. Інформаційний потік I являє собою безперервну або дискретну множину інформаційних об'єктів $I = \{i_n \mid n = \overline{1, N}\}$. Процес оцінювання гарантій включатиме два потоки: матеріальний – об'єкт експертизи TOE, і матеріально-інформаційний – сукупність (множину) свідоцтв E.

У нормативному документі [10] у якості об'єкта експертизи на відповідність вимогам гарантій постає засіб технічного захисту інформації від несанкціонованого доступу (НСД), який забезпечує, самостійно або у комплексі з іншими засобами, захист від загроз НСД до інформації, яка обробляється в ІТС. У стандартах [5; 9] об'єкт оцінювання визначений, як сукупність програмних, програмно-апаратних та апаратних засобів, які супроводжуються відповідними керівництвами.

У загальному випадку об'єкт експертизи (ОЕ) TOE можна представити у вигляді:

$$TOE =< Hw, Sw, D >, \quad (3)$$

де $Hw = \{Hw_i \mid i = \overline{1, I}\}$ – апаратні складові ОЕ;

$Sw = \{Sw_j \mid j = \overline{1, J}\}$ – програмні складові ОЕ;

$D = \{D_z \mid z = \overline{1, Z}\}$ – комплект документації до ОЕ.

Оцінювання ОЕ проводиться на підставі отриманих свідчень E. Основними джерелами свідчень є отримані від замовника експертизи документи та матеріали (програма та методика проведення експертизи), результати випробувань ОЕ (протокол випробувань), безпосередньо сам ОЕ та його складові. Отримана сукупність свідоцтв формально може бути представлена у вигляді множини $E = \{e_y \mid y = \overline{1, Y}\}$, а при наявності зв'язків успадкування (ієрархічних залежностей) – у вигляді графа G^E.

АК 5. Множина учасників – суб'єктів процесу. У загальному випадку, це:

$$PS =< Own, Man, Per, Sup, Cus >, \quad (4)$$

де Own – власник процесу;

Man – керівник процесу;

Per – виконавець процесу;

Sup – постачальник процесу;

Cus – споживач процесу.

Множина учасників процесу створюють команду $Team$, якщо на множині PS визначені ролі $role$ і повноваження $authority$ суб'єктів процесу, які характеризують відношення між учасниками процесу, тобто $Team\ (PS, role, authority)$.

В [10–12] суб'єктами експертизи визначені: юридичні і фізичні особи, які є замовниками експертизи; уповноважений державний орган; підрозділи уповноваженого державного органу, підприємства, заклади та організації, які проводять експертизу (організатори експертизи); фізичні особи – виконавці експертних робіт (експерти). У даному випадку суб'єкти можуть бути представлені у вигляді множини PS або графа G^{PS} [13].

Серед множини суб'єктів експертизи (оцінювання) головну роль відіграють експерти B, тобто особи, які приймають рішення відносно оцінювання властивостей гарантій (винесення вердиктів). Підбір експертів покладається на організаторів експертизи. Одним із методів підбору експертів є вибір за формальними ознаками, які в свою чергу можуть застосовуватися при порівнянні експертів. Для цього їх необхідно представити у вигляді множини:

$$B_i = \{b_{ix} \mid x = \overline{1, X}\}, \quad (5)$$

де X – кількість формальних ознак,

i – i -й експерт.

АК 6. Множина фінансових F, часових T, трудових L, економічних E, матеріальних Mat та інших ресурсів, необхідних для реалізації і виконання процесу Z:

$$Source = \{F, T, L, E, Mat\}. \quad (6)$$

Застосування наведених конструкцій *АК 1-АК 6* дозволяє представити наступну формалізовану модель процесу оцінювання гарантій:

$$Z =< Pur(G^P, V), d(A), F(TOE, E), IN \rightarrow OUT, Team(B), Source >. \quad (7)$$

Графічно дана модель представлена на рис. 1.

До результатів проведення експертизи висуваються вимоги об'єктивності, неупередженості, повторюваності, відтворюваності та співставленості. В контексті запропонованої моделі оцінювання гарантій інформаційної безпеки надамо формальні визначення вимог, що висуваються до результатів експертизи. Об'єктивність – властивість, яка визначає, що результати оцінювання гарантій безпеки повинні бути фактичними, тобто не підвладними впливу почуттів та думок експерта. Об'єктивність може бути забезпечена за умови, що результати оцінювання отримані шляхом дослідження наданих свідоцтв та у експерта є впевненість у достовірності цих свідоцтв.

Об'єктивність результатів тісно взаємопов'язана з вимогою неупередженості результатів оцінювання.

Неупередженість – властивість, яка передбачає, що оцінювання гарантій безпеки не повинне бути упередженим у відношенні будь-якого результату оцінювання. Неупередженість забезпечується незалежністю організаторів експертизи та експертів, які проводять оцінювання. Експерти не повинні бути причетними до організації-замовника експертизи та до розробників (розробки) об'єкта експертизи. Тобто експертами можуть бути лише ті люди (організації), для яких може бути документально підтверджено факт непричетності до будь-якої зі стадій розробки об'єкта оцінювання, обґрунтування та вибору певних проектних рішень. Отже, неупередженість досягається процедурою організації експертизи, що закріплена в нормативних документах.

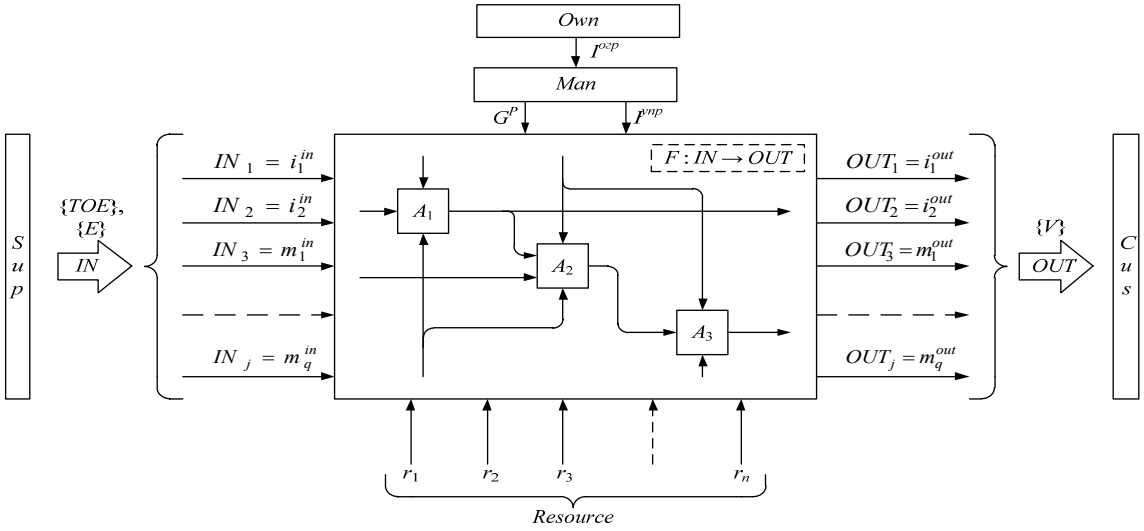

Рис. 1. Графічна інтерпретація моделі процесу оцінювання гарантій ІБ

Повторюваність – властивість, яка забезпечує ідентичність результатів оцінювання при повторному оцінюванні того ж самого об'єкту оцінювання, що проводиться за тією ж самою програмою та методикою оцінювання гарантій безпеки, тим самим експертом, з використанням тієї ж сукупності (множини) свідоцтв. У загальному випадку схема виконання вимоги повторюваності буде мати вигляд:

$Z_{(t_0,t_1)}$		$Z_{(t_2,t_3)}$	
(t_0,t_1)	$\neq$	(t_2,t_3)	– час проведення;
TOE_1	=	TOE_2	– об'єкт оцінювання;
PR_1	=	PR_2	– програма оцінювання;
A_1	=	A_2	– методика оцінювання;
B_1	=	B_2	– експерт;
E_1	=	E_2	– сукупність свідоцтв;
V_1	=	V_2	– результати оцінювання;

– номер експертизи;

В контексті даного визначення постає завдання порівняння окремих елементів моделі процесу оцінювання гарантій. Для вирішення цього завдання сформулюємо формальні умови порівняння елементів моделі.

Умова 1. Два об'єкта оцінювання TOE_1 та TOE_2 ідентичні, якщо виконується умова рівності множин їх складових:

$$\begin{aligned} &IF(\{Hw_i \mid i=\overline{1,I}\}_{TOE_1} = \{Hw_i \mid i=\overline{1,I}\}_{TOE_2}, \\ &\{Sw_j \mid j=\overline{1,J}\}_{TOE_1} = \{Sw_j \mid j=\overline{1,J}\}_{TOE_2}, \\ &\{D_z \mid z=\overline{1,Z}\}_{TOE_1} = \{D_z \mid z=\overline{1,Z}\}_{TOE_2}) THEN \\ &TOE_1 = TOE_2. \end{aligned} \quad (8)$$

Якщо при порівнянні двох об'єктів оцінювання умова рівності не виконується хоча б для однієї пари множин, то об'єкти оцінювання визнаються неідентичними.

Умова 2. Дві програми оцінювання PR_1 та PR_2 ідентичні, якщо виконується умова рівності графів $G^P_{PR_1} = G^P_{PR_2}$ та матриць їх суміжності

$$\begin{aligned} &(p_{ij})_{PR_1} = (p_{ij})_{PR_2}: \\ &IF(G^P_{PR_1} = G^P_{PR_2}, (p_{ij})_{PR_1} = (p_{ij})_{PR_2}, i=\overline{1,m}, \\ &j=\overline{1,n}) THEN\ PR_1 = PR_2. \end{aligned} \quad (9)$$

Якщо умова рівності не виконується, то програми визнаються різними.

Умова 3. Дві методики оцінювання A_1 та A_2 ідентичні, якщо виконується умова рівності графів $G^A_{A_1} = G^A_{A_2}$ та матриць їх суміжності

$$\begin{aligned} &(a_{ij})_{A_1} = (a_{ij})_{A_2}: \\ &IF(G^A_{A_1} = G^A_{A_2}, (a_{ij})_{A_1} = (a_{ij})_{A_2}, i=\overline{1,m}, \\ &j=\overline{1,n}) THEN\ A_1 = A_2. \end{aligned} \quad (10)$$

Якщо умова рівності не виконується, то методики визнаються різними.

Умова 4. Два експерта B_1 та B_2 ідентичні, якщо виконується умова рівності їх формальних ознак:

$$\begin{aligned} &IF(\{B_{1x} \mid x=\overline{1,X}\} = \{B_{2x} \mid x=\overline{1,X}\}) \\ &THEN\ B_1 = B_2. \end{aligned} \quad (11)$$

Якщо умова рівності не виконується, то експерти визнаються різними.

Умова 5. Дві сукупності свідоцтв E_1 та E_2 ідентичні, якщо виконується умова рівності множин:

$$\text{IF}(\{e_y \mid y=\overline{1,Y}\}_{E_1}=\{e_y \mid y=\overline{1,Y}\}_{E_2}) \text{ THEN } E_1=E_2, \quad (12)$$

або рівності графів та матриць їх суміжності:

$$\text{IF}(G^E_{E_1}=G^E_{E_2},(a_{ij})_{E_1}=(a_{ij})_{E_2},i=\overline{1,m}, j=\overline{1,n}) \text{ THEN } E_1=E_2. \quad (13)$$

Якщо умова рівності не виконується, то сукупності свідоцтв визнаються різними.

Умова 6. Два звіти V_1 та V_2 ідентичні, якщо виконується умова рівності множин значень лінгвістичних змінних відповідних звітів:

$$\text{IF}(\{L_i \mid i=\overline{1,I}\}_{V_1}=\{L_i \mid i=\overline{1,I}\}_{V_2}) \text{ THEN } V_1=V_2. \quad (14)$$

Якщо умова рівності не виконується, то звіти з оцінювання визнаються різними. Спираючись на умови 1–6 формально сформулюємо вимогу повторюваності.

Умова 7. Результати оцінювання гарантій вважаються повторюваними, якщо стосовно об'єкту оцінювання TOE було проведено дві експертизи (15) та (16)

$$Z_{(t_0,t_1)}=<\text{Pur}(PR_1,V_1),d(A_1),F(TOE_1,E_1), \text{IN}\rightarrow\text{OUT},\text{Team}(B_1),\text{Source}>, \quad (15)$$

$$Z_{(t_2,t_3)}=<\text{Pur}(PR_2,V_2),d(A_2),F(TOE_2,E_2), \text{IN}\rightarrow\text{OUT},\text{Team}(B_2),\text{Source}> \quad (16)$$

у проміжки часу (t_0,t_1) та (t_2,t_3) відповідно, виконуються умови:

– ідентичності об'єктів оцінювання $TOE_1=TOE_2$ (8);

– ідентичності програм оцінювання $PR_1=PR_2$ (9);

– ідентичності методик оцінювання $A_1=A_2$ (10);

– ідентичності експертів $B_1=B_2$ (11);

– ідентичності сукупності свідоцтв $E_1=E_2$ (12–13) та при цьому забезпечується умова ідентичності результатів експертизи $V_1=V_2$ (14).

Відтворюваність – властивість, яка забезпечує ідентичність результатів оцінювання при повторному оцінюванні того ж самого об'єкту оцінювання, що проводиться за тією ж самою програмою та методикою оцінювання гарантій безпеки, різними експертами, з використанням тієї ж сукупності (множини) свідоцтв.

Умова 8. Результати оцінювання гарантій вважаються відтворюваними, якщо стосовно об'єкту оцінювання TOE було проведено дві експертизи (15) та (16) у проміжки часу (t_0,t_1) та (t_2,t_3) відповідно, виконуються умови: ідентичності об'єктів оцінювання $TOE_1=TOE_2$ (8), ідентичності програм оцінювання $PR_1=PR_2$ (9), ідентичності методик оцінювання $A_1=A_2$ (10), неідентичності експертів $B_1\neq B_2$ (11), ідентичності сукупності свідоцтв $E_1=E_2$ (12–13) та при цьому забезпечується умова ідентичності результатів експертизи $V_1=V_2$ (14).

Співставленість – властивість, яка забезпечує порівнянність результатів оцінювання, що отримані при оцінюванні того ж самого об'єкту оцінювання, що проводиться за різними програмами та методиками оцінювання гарантій безпеки різними (або тими ж) експертами.

Умова 9. Результати оцінювання гарантій вважаються співставленими, якщо стосовно об'єкту оцінювання TOE було проведено дві експертизи (15) та (16) у проміжки часу (t_0,t_1) та (t_2,t_3) відповідно, виконуються умови:

– ідентичності об'єктів оцінювання $TOE_1=TOE_2$ (8);

– неідентичності програм оцінювання $PR_1\neq PR_2$ (9);

– неідентичності методик оцінювання $A_1\neq A_2$ (10), ідентичності або неідентичності експертів $B_1=(\neq)B_2$ (11);

– ідентичності або неідентичності сукупності свідоцтв $E_1=(\neq)E_2$ (12–13) та при цьому забезпечується умова порівняності результатів експертизи $V_1(L_i)=V_2(L_i)$ (14).

Висновки

У роботі запропонована формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації, яка може розглядатися як базова та застосовуватись для подальших досліджень процесу оцінювання гарантій інформаційної безпеки.

Розроблено умови ідентичності об'єктів оцінювання, програм оцінювання, методик оцінювання експертів, сукупності свідоцтв та результатів оцінювання.

В рамках розроблених умов в роботі вперше запропоновані формальні умови повторюваності, відтворюваності та співставленості результатів оцінювання.

Дані умови є чіткими та спираються на суворі рівності відповідних множин чи графів, що дозволяє на практиці об'єктивно підтвердити виконання вимог до результатів експертизи.

Список літератури

1. Potii O. Advanced security assurance case based on ISO/IEC 15408 / O. Potii, O. Illiashenko, D. Komin // Theory and Engineering of Complex Systems and Dependability. – 2015. – P. 391-401.

2. Лемешко А.В. Категориально-тензорное представление телекоммуникационной системы / А.В. Лемешко, О.Ю. Евсеева, А.В. Чечуй // Наукові записки УНДІЗ. – 2008. – № 2(4). – С. 3-15.

3. Potij A.V. A Method of Evaluating Assurance Requirements / A.V. Potij, D.S. Komin, I.N. Rebriy // Information & Security. An International Journal. – 2012. – Vol. 28, No. 1. – P. 108-120.

4. Ілляшенко О.О. Оцінювання інформаційної безпеки систем на програмовній логіці з використанням кейсів: таксономія, нотація, концепція / О.О. Ілляшенко // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 2(31). – С. 97–103. https://doi.org/10.30748/nitps.2018.31.12.

5. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT).

6. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT).

7. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT).

8. Потий А.В. Формальная модель процесса защиты информации / А.В. Потий // Радіоелектронні і комп'ютерні системи. – 2006. – № 5(17). – С. 128-133.

9. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (ISO/IEC 18045:2008, IDT).

10. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах : НД ТЗІ 2.6-001-11. – [Чинний від 2011-03-25]. – К.: Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2011. – 104 с. – (Нормативний документ системи технічного захисту інформації).

11. ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model [Elektronik resource]. – Available at: https://www.iso.org/standard/50341.html.

12. ISO/IEC 15408-3:2008, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement [Elektronik resource]. – Available at: https://www.iso.org/standard/46413.html.

13. Prieto-Diaz R. The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities / R. Prieto-Diaz // Commonwealth Information Security Center Technical Report CISC-TR-2002-03. – December 2002. – CISC, James Madison University, USA. – 62 p.

References

1. Potii, O., Illiashenko, O. and Komin, D. (2015), Advanced security assurance case based on ISO/IEC 15408, *Theory and Engineering of Complex Systems and Dependability*, pp. 391-401.

2. Lemeshko, O.V., Evseeva, O.U. and Chechui, O.V. (2008), "Kategoryalno-tenzornoe predstavlenye telekommunykacionnoj sistemu" [Categorical-tensor representation of the telecommunication system], *Scientific proceeding of Ukrainian research institute of communication*, Kyiv, No. 2(4), pp. 3-15.

3. Potij, A.V., Komin, D.S. and Rebriy, I.N. (2012), A Method of Evaluating Assurance Requirements, *Information & Security*, *An International Journal*, No. 28, pp. 108-120.

4. Illiashenko, O.O. (2018), "Ocinjuvannja informacijnoji bezpeky system na proghramovnij loghici z vykorystannjam kejsiv: taksonomija, notacija, koncepcija" [Estimation of information security of systems on programmable logic using cases: taxonomy, notation, concept], *Science and Technology of the Air Forces of Ukraine*, No. 2(31), pp. 97-103. https://doi.org/10.30748/nitps.2018.31.12.

5. The State Standard of Ukraine (2017), "*ISO/IEC 15408-1 (ISO/IEC 15408-1:2009, IDT) Informacijni texnologiyi. Metody zaxystu. Kryteriyi ocinky. Chastyna 1. Vstup ta zagalna model*" [*Informational technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model*].

6. The State Standard of Ukraine (2017), "*ISO/IEC 15408-2 (ISO/IEC 15408-2:2008, IDT) Informacijni texnologiyi. Metody zaxystu. Kryteriyi ocinky. Chastyna 2. Funkcionalni vymogy*" [*Informational technology. Security techniques. Evaluation criteria for IT security. Part 2: Functional requirements*].

7. The State Standard of Ukraine (2017), "*ISO/IEC 15408-3 (ISO/IEC 15408-3:2008, IDT) Informacijni texnologiyi. Metody zaxystu. Kryteriyi ocinky. Chastyna 3. Vymogy do garantiyi bezpeky*" [*Informational technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance requirement*].

8. Potij, A.V. (2006), "Formalnaya model processa zashhytu ynformacyy" [Formal model of the information security process], *Radio electronic and computer systems*, No. 5 (17), pp.128-133.

9. The State Standard of Ukraine (2015), "*ISO/IEC 18045 (ISO/IEC 18045:2008, IDT) Informacijni texnologiyi. Metody zaxystu. Metodologiya ocinyuvannya bezpeky informacijnyx texnologij*" [*Information Technology. Methods of protection. Methodology for IT security assessment*].

10. Administration of the State Service for Special Communications and Information Protection of Ukraine (2011), ND 2.6-001 "*Poryadok provedennya robit z derzhavnoyi ekspertyzy zasobiv texnichnogo zaxystu informaciyi vid nesankcionovanogo dostupu ta kompleksnyx system zaxystu informaciyi v informacijno-telekomunikacijnyx systemax*" [*Procedure for conducting*

works on state expertise of means of technical protection of information from unauthorized access and complex systems of information security in information and telecommunication systems], Kyiv, 104 p.

11. "ISO/IEC 15408-1 (2009), *Informational technology. Security techniques. Evaluation criteria for IT security. Part 1*: *Introduction and general model*, available at: https://www.iso.org/standard/50341.html

12. ISO/IEC 15408-3 (2008), Informational technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance requirement, available at: https://www.iso.org/standard/46413.html

13. Prieto-Diaz, R. (2002), The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities, *Commonwealth Information Security Center Technical Report CISC-TR*, *December 2002*, James Madison University, USA, 62 p.

Надійшла до редколегії 11.10.2018
Схвалена до друку 5.11.2018

Відомості про авторів:

Комін Дмитро Сергійович
кандидат технічних наук
старший викладач
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-4439-346X

Чечуй Олександр Вікторович
кандидат технічних наук доцент
доцент кафедри
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-7584-4457

Левченко Михайло Анатолійович
кандидат військових наук доцент
начальник кафедри
інституту авіації
та протиповітряної оборони
Національного університету оборони України
ім. І. Черняховського, Київ, Україна
https://orcid.org/0000-0003-1872-2960

Панхохін Олександр Сергійович
Бакалавр
курсант
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-2163-3558

Павловський Володимир Анатолійович
Бакалавр
курсант
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-3173-2584

Information about the authors:

Dmytro Komin
Candidate of
Technical Sciences
Senior Instructor of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-4439-346X

Oleksandr Chechui
Candidate of Technical Sciences
Associate Professor
Senior Lecturer of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-7584-4457

Mykhailo Levchenko
Candidate of Military Sciences Associate Professor
Head of Department
of Institute of Aviation
and Air Defense of Ivan Chernyakhovsky
National Defense University of Ukraine,
Kyiv, Ukraine
https://orcid.org/0000-0003-1872-2960

Olexander Pankhokhin
Bachelor
Cadet
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-2163-3558

Volodymyr Pavlovskyi
Bachelor
Cadet
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-3173-2584

ФОРМАЛЬНАЯ МОДЕЛЬ ОЦЕНКИ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Д.С. Комин, А.В.Чечуй, М.А. Левченко, О.С. Панхохин, В.А. Павловский

Рассмотрены особенности проведения оценки гарантий информационной безопасности для комплексной системы защиты информации в соответствии с государственными и международными стандартами. Предложено применение формальной модели оценки требований гарантий информационной безопасности для субъектов экспертизы с применением аксиоматических конструкций. Такая модель позволяет осуществлять исследования процесса оценки гарантий информационной безопасности и определять требования к результатам экспертизы относительно повторяемости, воспроизводимости, сопоставимости. объективности и беспристрастности.

Также в статье для определения требований, которые предъявляются к результатам экспертизы, предложены условия идентичности объектов оценивания, программ и методик оценивания, экспертов, совокупности свидетельств и результатов оценивания. Данные условия являются четкими и опираются на строгие определения равенства соответствующих множеств или графов, что позволяет на практике объективно подтвердить выполнение требований к результатам экспертизы.

Ключевые слова: *комплексная система защиты информации, информационно-телекоммуникационная система, информационная безопасность, субъект экспертизы, объект экспертизы, формальная модель, эксперт.*

FORMALIZED MODEL OF ASSESSMENT OF INFORMATION SECURITY GUARANTEES OF THE INTEGRATED INFORMATION SECURITY SYSTEM

D. Komin, O. Chechui, M. Levchenko, A. Pankhokhin, V. Pavlovskyi

In the article, the peculiarities of evaluating information security guarantees for the integrated information security system in accordance with state and international standards are considered. The application of the formalized model of the process which assessing the requirements of guarantees of information security for the subjects of expertise by using the axiomatic constructions is proposed. The following aspects were taken into account when developing a model of assessment of information security guarantees: functional, informative, organizational and causal characteristics. The functional characteristic of the model accurately determines what is carried out by the elements of the process. The information characteristic of the model reflects the informational nature that is being formed, produced or used by the process. Organizational characteristic of the model describes who and when performs specific actions, work, operations of the process with the inclusion of physical mechanisms of transmission and storage of object. The causal characteristic of the model refers to the coordination and dependence of the actions and the subjects of these actions. Such model allows to study the process of assessing information security guarantees and to determine the requirements for the results of the examination, regarding impartiality, objectivity, repeatability, reproducibility and comparability. Also, the article defines the requirements for the results of the examination and proposes conditions for the identity of the objects of assessment, programs and methods of assessment, experts, evidence and evaluation results. These conditions are clear and rely on strict definitions of the equality of the corresponding sets or graphs, which allows in practice to objectively confirm the fulfillment of the requirements for the results of the examination.

Keywords*: integrated information security system, information and telecommunication system, information security subject of expertise object of expertise, formalized model, expert.*