DOI: 10.18372/2410-7840.19.11499
УДК 004.056.5:343.326 (045)

МУЛЬТИРІВНЕВА МОДЕЛЬ ДАНИХ ДЛЯ ІДЕНТИФІКАЦІЇ ЗАБЕЗПЕЧЕНОСТІ ВИМОГ ВІДПОВІДНО НОРМАТИВНО-ПРАВОВОМУ ЗАБЕЗПЕЧЕННЮ КІБЕРБЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

Володимир Харченко, Олександр Корченко, Сергій Гнатюк

Захист критичної інфраструктури на сьогодні є одним із першочергових завдань держави, особливо гостро це питання постає перед державами, які впроваджують новітні інформаційно-комунікаційні технології в усіх критичних галузях. Зазначені технології, крім іншого, породжують цілу низку нових уразливостей та потенційних кіберзагроз. У галузі цивільної авіації рівень критичності значно підсилюється комунікацією та взаємодією між наземними системами і повітряними суднами. Відома модель формування вимог до забезпечення кібербезпеки цивільної авіації дозволяє формалізувати процес створення повної множини вимог, які необхідно забезпечити для захисту цивільної авіації від кіберзагроз, проте відсутній механізм визначення забезпеченості певних режимів безпеки внаслідок реалізації методів та засобів, задекларованих у відповідних вимогах. З огляду на це, актуальною є розробка підходу до визначення забезпеченості режимів безпеки, що враховуватимуть додаткові характеристики безпеки. У цій роботі запропоновано мультирівневу модель даних, яка за рахунок використання базової моделі формування вимог до забезпечення кібербезпеки цивільної авіації, конкатенації бінарних послідовностей, що характеризують режими безпеки, та бінарно-шістнадцяткового кодового представлення характеристик безпеки, множини моделей безпеки та підмножин характеристик безпеки (з урахуванням додаткових характеристик), дозволяє формалізувати процес ідентифікації забезпеченості вимог та визначення режимів безпеки критичних авіаційних інформаційних систем. У подальших дослідженнях планується розробити метод оцінювання повноти забезпечення вимог у результаті реалізації відповідних методів та засобів захисту.

Ключові слова: *кібербезпека, цивільна авіація, критична інформаційна авіаційна система, модель ідентифікації, нормативно-правове забезпечення, модель безпеки, характеристика безпеки.*

Вступ

Сучасне вітчизняне законодавство у сфері захисту критичної інфраструктури знаходиться на стадії свого формування – поки що відсутній перелік об'єктів критичної інфраструктури, проте визначено категорії об'єктів, для яких встановлюються особливі умови забезпечення їх захисту [1], зокрема підприємства, які мають стратегічне значення для економіки та безпеки держави; особливо важливі об'єкти електроенергетики; особливо важливі об'єкти нафтогазової галузі; важливі державні об'єкти, у тому числі пункти управління органів державної влади та органів місцевого самоврядування; об'єкти можливих терористичних посягань; об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за відповідними договорами; об'єкти підвищеної небезпеки (у т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу); об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів; радіаційно небезпечні об'єкти, для яких розробляється об'єктова проектна загроза; об'єкти, які віднесені до категорій з цивільного захисту; об'єкти, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту; аварійно-рятувальні служби; Національна система конфіденційного зв'язку; платіжні системи; нерухомі об'єкти культурної спадщини тощо.

Аналіз існуючих досліджень і постановка завдання

Одним з останніх вітчизняних нормативних документів щодо захисту критичної інфраструктури є Постанова КМУ № 563 від 23 серпня 2016 року «Про затвердження Порядку формування переліку інформаційно-телекомунікацій-них систем об'єктів критичної інфраструктури держави», яка визначає порядок формування пропозицій до зазначеного переліку з боку стейкхолдерів, визначає перелік базових термінів, а також перелік негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему (ІТС), серед яких: 1) виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону); 2) негативний вплив на стан енергетичної безпеки держави (регіону); 3) негативний вплив на стан економічної безпеки держави; 4) негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі;

5) негативний вплив на систему управління державою; 6) негативний вплив на суспільно-політичну ситуацію в державі; 7) негативний вплив на імідж держави; 8) порушення сталого функціонування фінансової системи держави; 9) порушення сталого функціонування транспортної інфраструктури держави (регіону); 10) порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав.

Відповідно до міжнародного досвіду (наприклад, [2]), серед важливих об'єктів критичної інфраструктури варто відзначити інфраструктуру ІТС, нафто- та газотранспортну системи, фінансову, енергетичну та транспортну галузі (рис. 1). Несанкціоноване втручання у роботу останньої може призвести до значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури [3].

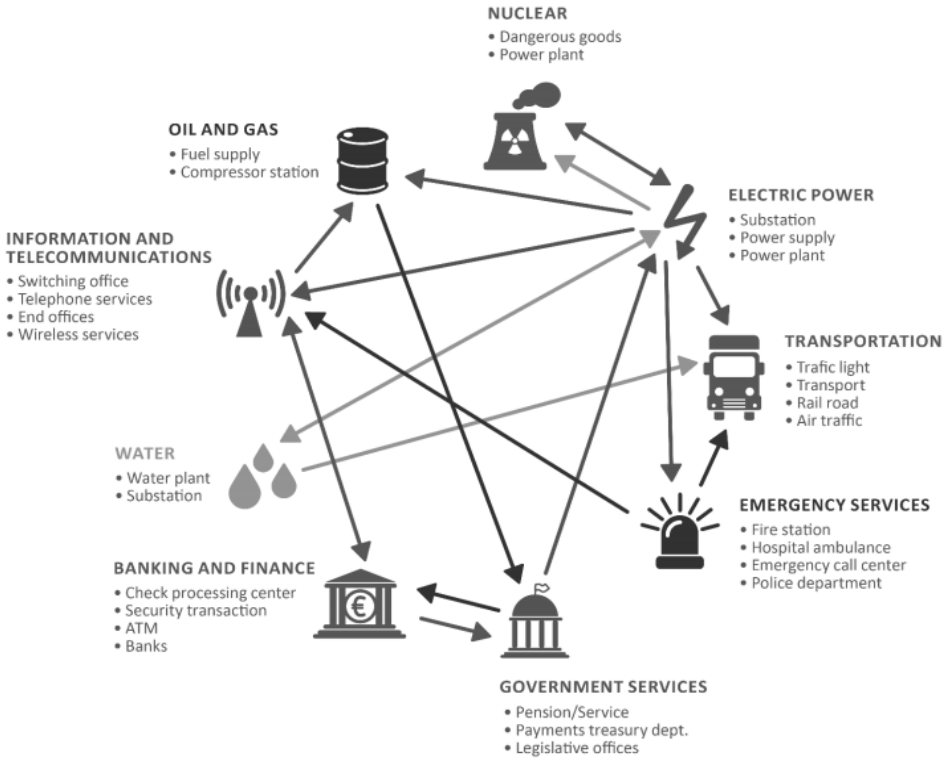


Рис. 1. Критична інфраструктура згідно даних European Union Agency for Network and Information Security [2]

Несанкціонований доступ і використання критичних авіаційних інформаційних систем (КАІС) [4] може призвести до виникнення загроз безпеці пасажирів, екіпажу та наземного персоналу, з огляду на що важливим є забезпечення їх кібербезпеки (КБ) [5, 6] шляхом захисту від несанкціонованого втручання, попередження втручання в роботу КАІС, виявлення кібератак на них тощо. Більшість відомих робіт у цьому напрямку є орієнтованими на розробку або загальних підходів до забезпечення КБ, або створення методів, моделей та засобів щодо забезпечення конфіденційності, цілісності й доступності інформації (без врахування додаткових характеристик безпеки), що обробляється, зберігається чи передається за допомогою сучасних інформаційно-комунікацій-них технологій. Таким чином, відповідно до поточного стану досліджень, не в повній мірі враховуються сучасні вимоги, задекларовані в керівних документах щодо безпеки цивільної авіації (ЦА), та специфіка діяльності ЦА, а також не використовуються моделі кібербезпеки (МКБ), які враховують додаткові характеристики безпеки. З огляду на це, **метою** роботи є розробка, на базі відомого підходу до формування вимог, мультирівневої моделі, яка враховує найбільш сучасні підходи до захисту критичної інфраструктури і дозволяє ідентифікувати забезпеченість вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації.

Основна частина дослідження

У статті [7] запропоновано базову модель формування вимог до забезпечення КБ ЦА (1), яка за рахунок введення базової множини вимог, які містяться у різних керівних документах щодо безпеки

ЦА, та відповідних підмножин, що характеризують базову множину (підмножини наборів вимог відповідних керівних органів, підмножини наборів вимог i-го керівного органу), дає можливість формалізувати процес створення повної множини вимог, які необхідно забезпечити для захисту ЦА від кіберзагроз.

$$\mathbf{R} = \{\bigcup_{i=1}^{n}\mathbf{R}_i\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{R}_{ij}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_{ij}}R_{ijk}\}\}\} =$$
$$= \{\{\{R_{111}, R_{112}, ..., R_{11r_{11}}\}, \{R_{121}, R_{122}, ..., R_{12r_{12}}\}, ..., \{R_{1m_11}, R_{1m_12}, ..., R_{1m_1r_{nm_1}}\}\},$$
$$\{\{R_{211}, R_{212}, ..., R_{21r_{21}}\}, \{R_{221}, R_{222}, ..., R_{22r_{22}}\}, ..., \{R_{2m_21}, R_{2m_22}, ..., R_{2m_2r_{nm_2}}\}\}, ...,$$
$$\{\{R_{n11}, R_{n12}, ..., R_{n1r_{n1}}\}, \{R_{n21}, R_{n22}, ..., R_{n2r_{n2}}\}, ..., \{R_{nm_11}, R_{nm_12}, ..., R_{nm_nr_{nm_n}}\}\}\}, \quad (1)$$

де $\mathbf{R}_i \subseteq \mathbf{R}$ $(i = \overline{1,n})$ – підмножини наборів вимог відповідних керівних органів; n – загальна кількість вимог відповідних керівних органів; $\mathbf{R}_{ij}$ $(i = \overline{1,n}$, $j = \overline{1,m_i})$ – підмножини наборів вимог i-го керівного органу; m_i – кількість вимог i-го керівного органу; R_{ijk} $(i = \overline{1,n}$, $j = \overline{1,m_i}$, $k = \overline{1,r_{ij}})$ – вимоги з підмножини набору вимог $\mathbf{R}_{ij}$; r_{ij} – кількість таких вимог у кожній з множин ij-го набору. Наприклад, для множини вимог щодо забезпечення КБ ЦА України $\mathbf{R} = \mathbf{R}_{civil\_aviation\_ua}$, використовуючи (1) та (3-5) у [7], при $i = \overline{1,n}$, $j = \overline{1,m_i}$, $n = 3$, $m_1 = 4$, $m_2 = 1$, $m_3 = 2$, $r_{11} = r_{31} = 5$, $r_{12} = r_{32} = 4$, $r_{13} = 7$, $r_{14} = 6$, $r_{21} = 13$, матимемо:

$$\mathbf{R} = \mathbf{R}_{civil\_aviation\_ua} = \{\bigcup_{i=1}^{3}\mathbf{R}_i\} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\mathbf{R}_{ij}\}\} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_{ij}}R_{ijk}\}\}\} =$$
$$= \{\{\{R_{111}, R_{112}, ..., R_{115}\}, \{R_{121}, R_{122}, ..., R_{124}\}, \{R_{131}, R_{132}, ..., R_{137}\}, \{R_{141}, R_{142}, ..., R_{146}\}\},$$
$$\{\{R_{211}, R_{212}, ..., R_{21,13*}\}\}, \{\{R_{311}, R_{312}, ..., R_{315}\}, \{R_{321}, R_{322}, ..., R_{324}\}\}\} =$$
$$= \{\{\{R_{ICAO_{11}}, R_{ICAO_{12}}, ..., R_{ICAO_{15}}\}, \{R_{ICAO_{21}}, R_{ICAO_{22}}, ..., R_{ICAO_{24}}\}, \{R_{ICAO_{31}}, R_{ICAO_{32}}, ..., R_{ICAO_{37}}\}, \{R_{ICAO_{41}}, R_{ICAO_{42}}, ..., R_{ICAO_{46}}\}\},$$
$$\{\{R_{ECAC_{11}}, R_{ECAC_{12}}, ..., R_{ECAC_{1,13}}\}\}, \{\{R_{NATIONAL_{11}}, R_{NATIONAL_{12}}, ..., R_{NATIONAL_{15}}\}, \{R_{NATIONAL_{21}}, R_{NATIONAL_{22}}, ..., R_{NATIONAL_{24}}\}\}\} =$$
$$= \{\{\{AR_1, AR_2, ..., AR_5\}, \{VR_1, VR_2, ..., VR_4\}, \{PC_1, PC_2, ..., PC_7\}, \{ATC_1, ATC_2, ..., ATC_6\}\},$$
$$\{\{SC_1, SC_2, ..., SC_{13}\}\}, \{\{OR_1, OR_2, ..., OR_5\}, \{TR_1, TR_2, ..., TR_4\}\}\},$$

де $R_{111} = R_{ICAO_{11}} = AR_1$, $R_{112} = R_{ICAO_{12}} = AR_2$, …, $R_{115} = R_{ICAO_{15}} = AR_5$, $R_{121} = R_{ICAO_{21}} = VR_1$, $R_{122} = R_{ICAO_{22}} = VR_2$, …, $R_{124} = R_{ICAO_{24}} = VR_4$, $R_{131} = R_{ICAO_{31}} = PC_1$, $R_{132} = R_{ICAO_{32}} = PC_2$, …, $R_{137} = R_{ICAO_{37}} = PC_7$, $R_{141} = R_{ICAO_{41}} = ATC_1$, $R_{142} = R_{ICAO_{42}} = ATC_2$, …, $R_{146} = R_{ICAO_{46}} = ATC_6$, $R_{211} = R_{ECAC_{11}} = SC_1$, $R_{212} = R_{ECAC_{12}} = SC_2$, …, $R_{21,13} = R_{ECAC_{1.13}} = SC_{13}$, $R_{311} = R_{NATIONAL_{11}} = OR_1$, $R_{312} = R_{NATIONAL_{12}} = OR_2$, …, $R_{315} = R_{NATIONAL_{15}} = OR_5$, $R_{321} = R_{NATIONAL_{21}} = TR_1$, $R_{322} = R_{NATIONAL_{22}} = TR_2$, …, $R_{324} = R_{NATIONAL_{24}} = TR_4$ – елементи базової множини, які відображають вимоги щодо забезпечення КБ ЦА України відповідно до вимог керівних органів, що містяться у нормативних документах [8-11].

На основі відповідних елементів базової множини сформуємо вимоги, на основі яких будується відповідна таблиця (див. табл. 1), де # – номер статті (пункту, підпункту) відповідного керівного документу; $R_{111}...R_{ijk}$ *description* – опис вимог (лінгвістичне представлення) щодо забезпечення КБ ЦА. Для прикладу, використовуючи вимоги керівних органів [8-11], а також табл. 1-3 [7], таблиця вимог щодо забезпечення КБ ЦА України на основі табл. 1 матиме вигляд, представлений у табл. 2.

Таблиця 1

Вимоги керівних органів щодо захисту ЦА від кіберзагроз (загальний вигляд)

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} (при $i = \overline{1,n}$, $j = \overline{1,m_i}$, n, m_i, r_{ij})	*Article point*	R_{ijk} *code*
$\mathbf{R}_1 \dots \mathbf{R}_n$	$\mathbf{R}_{11}...\mathbf{R}_{nm_n}$	$R_{111}...R_{ijk}$ *description*	#	$R_{111}...R_{nm_nr_{nm_n}}$

Таблиця 2

Вимоги керівних органів щодо захисту ЦА України від кіберзагроз

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} (при $i=\overline{1,n}$, $j=\overline{1,m_i}$, $n=3$, $m_1=4$, $m_2=1$, $m_3=2$, $r_{11}=r_{31}=5$, $r_{12}=r_{32}=4$, $r_{13}=7$, $r_{14}=6$, $r_{21}=13$)	*Article point* [8-11]	R_{ijk} *code*
ICAO$_1$	DOC 8973/8 18.1.6.a **Адміністративне регулювання (AR)**	Стандарти, політика і процедури забезпечення безпеки	18.1.6.a.1	AR_1
		Відбір, підготовка та перепідготовка персоналу (у т.ч. на керівні посади)	18.1.6.a.2	AR_2
		Оцінка загроз та ризиків з метою визначення уразливостей КАІС і ймовірності атаки	18.1.6.a.3	AR_3
		Контроль якості послуг, включаючи перевірки та інспекції	18.1.6.a.4	AR_4
		Безпека ланцюга поставки ПЗ та обладнання	18.1.6.a.5	AR_5
ICAO$_2$	DOC 8973/8 18.1.6.b **Віртуальне регулювання (VR)**	Засоби мережевого захисту	18.1.6.b.1	VR_1
		Засоби криптографічного захисту даних	18.1.6.b.2	VR_2
		Системи виявлення / попередження вторгнень до КАІС	18.1.6.b.3	VR_3
		Системи антивірусного захисту та протидії шкідливому ПЗ	18.1.6.b.4	VR_4
ICAO$_3$	DOC 8973/8 18.1.6.c **Фізичний контроль (PC)**	Захист обладнання та контроль доступу до нього	18.1.6.c.1	PC_1
		Аутентифікація легітимних користувачів КАІС	18.1.6.c.2	PC_2
		Обмеження кола осіб, що мають доступ до ресурсів КАІС	18.1.6.c.3	PC_3
		Чітка пропускна система	18.1.6.c.4	PC_4
		Постійний контроль та управління доступом до КАІС	18.1.6.c.5	PC_5
		Використання автономних резервних систем	18.1.6.c.6	PC_6
		Ведення журналів реєстрації операцій та експлуатаційних параметрів	18.1.6.c.7	PC_7
ICAO$_4$	DOC 9985/1 Додаток B **Контроль повітряного руху (ATC)**	Визначення переліку КАІС	Дод.B.3.2	ATC_1
		Захист КАІС від НСД	Дод.B.3.3	ATC_2
		Попередження вторгнень у роботу КАІС	Дод.B.3.3	ATC_3
		Виявлення атак на КАІС	Дод.B.3.3	ATC_4
		Застосування процедур оцінювання ризиків	Дод.B.3.5	ATC_5
		Оцінювання уразливостей та наслідків відмов КАІС	Дод.B.3.6	ATC_6
ECAC$_1$	14.1 **Контроль на безпеку (SC)**	Застосування заходів безпеки до КАІС	14.1.1	SC_1
		Включення КАІС до процесу оцінки загроз	14.1.2	SC_2
		Відділення КАІС від публічних мереж	14.1.3	SC_3
		Мінімізація підключень до КАІС і контроль доступу	14.1.3	SC_4
		Відбір, підготовка та перепідготовка операторів, що обслуговують КАІС	14.1.4	SC_5
		Координація й узгодження заходів щодо захисту КАІС з існуючими заходами щодо авіаційної безпеки	14.1.4	SC_6
		Врахування заходами захисту форми, впровадження, управління й застосування нових КАІС	14.1.5	SC_7
		Використання заходів захисту прийнятного рівня в уже існуючих КАІС	14.1.5	SC_8
		Забезпечення прийнятних заходів безпеки до апаратного та програмного забезпечення, що використовується в КАІС	14.1.6	SC_9
		Безпека ланцюга поставки апаратних і програмних засобів КАІС	14.1.6	SC_{10}
		Забезпечення віддаленого доступу до КАІС за узгоджених і безпечних умов	14.1.7	SC_{11}
		Виключення можливості несанкціонованого доступу постачальників після купівлі КАІС	14.1.7	SC_{12}
		Ведення обліку й оцінки кібератак на КАІС	14.1.8	SC_{13}
NATIONAL$_1$	174 **Організаційні вимоги (OR)**	Визначення пріоритетів державної політики в сфері протидії КЗ у ЦА	174.a1	OR_1
		Державний нагляд за станом захисту КАІС від КЗ	174.a2	OR_2
		Включення КАІС до процесу оцінки загроз ЦА	174.a3	OR_3
		Ідентифікація КАІС, збір, узагальнення та облік даних	174.a4	OR_4
		Впровадження системи відбору, перевірки та підготовки фахівців з питань протидії КЗ у ЦА	174.a5	OR_5
NATIONAL$_2$	175 **Технічні вимоги (TR)**	Визначення повного переліку КАІС	175.a1	TR_1
		Створення моделі загроз для кожної КАІС	175.a2	TR_2
		Реалізація технічного захисту КАІС	175.a3	TR_3
		Контроль за ефективністю заходів захисту	175.a4	TR_4

Для ідентифікації забезпеченості вимог щодо захисту ЦА від кіберзагроз введемо відповідну множину всіх МКБ $\mathbf{M}$:

$$\mathbf{M} = \{\bigcup_{i=1}^{q} \mathbf{M}_i\} = \{\mathbf{M}_1, \mathbf{M}_2 \ldots \mathbf{M}_q\}, \quad (2)$$

де $\mathbf{M}_i \subseteq \mathbf{M}$ $(i = \overline{1,q})$ – моделі визначення КБ; q – загальна кількість зазначених МКБ, а

$$\mathbf{M}_i = \{\bigcup_{j=1}^{p_i} M_{ij}\} = \{M_{i1}, M_{i2} \ldots M_{ip_i}\}, \quad (3)$$

при чому M_{ij} $(i = \overline{1,q},\ j = \overline{1,p_i})$ – характеристики, що використовуються в i-й МКБ; p_i – кількість характеристик безпеки i-ї МКБ. З урахуванням (3) вираз (2) можна представити у наступному вигляді:

$$\mathbf{M} = \{\bigcup_{i=1}^{q} \mathbf{M}_i\} = \{\bigcup_{i=1}^{q} \{\bigcup_{j=1}^{p_i} M_{ij}\}\} = \{\{M_{11}, M_{12}, ..., M_{1p_1}\}, \{M_{21}, M_{22}, ..., M_{2p_2}\}, ..., \{M_{q1}, M_{q2}, ..., M_{qp_n}\}\}, \ (i = \overline{1,q},\ j = \overline{1,p_i}). \quad (4)$$

Наприклад, для ЦА як для складової критичної інфраструктури держави (рис. 1), доцільно застосовувати розширені МКБ, зокрема замість базової моделі Тріада CIA (вона ж Тріада КЦД) (рис. 2а) варто використовувати моделі, які враховують, крім базових, ще й додаткові характеристики безпеки. Серед сучасних МКБ, що враховують додаткові характеристики, відносяться Гексада Паркера (рис. 2б) [12], модель STRIDE (рис. 2в) [13] та Модель 5А (рис. 2г) [14].

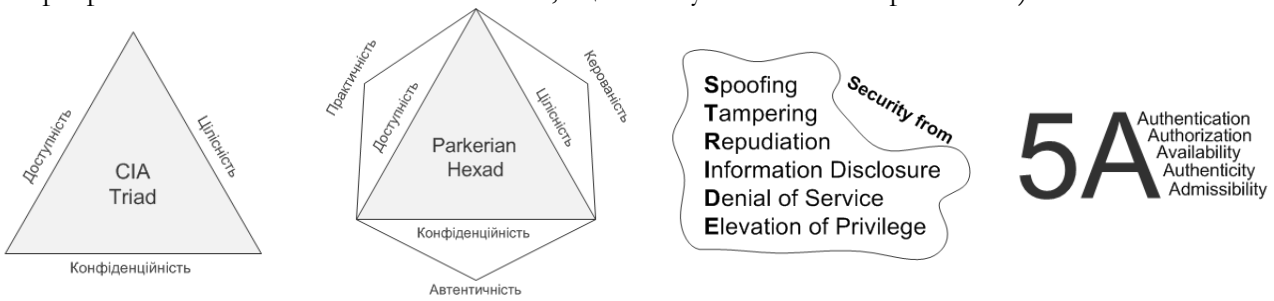
У цьому випадку, наприклад, при $q = 3$ згідно виразу (2), можна сформувати множину МКБ $\mathbf{M}$, яка, з урахуванням найбільш сучасних підходів до захисту критичної інфраструктури держави, складається з трьох множин:

$$\mathbf{M} = \mathbf{M}_{CIIP} = \{\bigcup_{i=1}^{3} \mathbf{M}_i\} = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3\} = \{\mathbf{M}_{PH}, \mathbf{M}_{STRIDE}, \mathbf{M}_{A5}\} = \{\mathbf{PH}, \mathbf{STRIDE}, 5\mathbf{A}\}. \quad (5)$$

Гексада Паркера (рис. 2б) [12] є однією з найбільш популярних альтернатив Тріаді КЦД (рис. 2а), що була запропонована Д. Паркером в 1998 році в роботі «Боротьба з комп'ютерною злочинністю». У гексаді Паркера визначено шість характеристик безпеки, в число яких, крім конфіденційності, цілісності та доступності, входять ще три – автентичність (користувач не може видати себе за іншого, а документ завжди має достовірну інформацію про його автора), керованість (фізичний контроль над пристроєм або іншим середовищем зберігання інформації надається тільки тим, хто має на це право) та практичність (зручність практичного використання як власне інформації, так і процедур, пов'язаних з її обробкою та підтримкою).

Модель STRIDE (рис. 2в) [13] використовується компанією Microsoft при розробці безпечного програмного забезпечення. Вважається, що ця модель розширює тріаду КЦД і дозволяє розробнику поглянути на інформаційну систему з точки зору порушника КБ. Відповідно до цієї моделі інформація (ресурс, актив) знаходиться в безпеці, якщо вона захищена від підміни даних, зміни даних (аналог цілісності), відмови від відповідальності, розголошення інформації (аналог конфіденційності), відмови в обслуговуванні (аналог доступності) та захоплення привілеїв.

Модель 5А (рис. 2г) [14], запропонована Б. Шнайєром, містить такі характеристики безпеки як аутентифікація (ким є користувач?), авторизація (які повноваження має користувач?), доступність (чи може користувач отримати можливість роботи з інформацією (даними)?), автентичність (чи не пошкоджені дані порушником?) та допустимість (чи є інформація (дані) достовірними, актуальними та корисними?).



а *б* *в* *г*

Рис. 2. Сучасні МКБ: а) Тріада CIA; б) Гексада Паркера; в) STRIDE; г) 5А

Далі, використовуючи послідовно (3) та (4) для Гексади Паркера, наприклад, при $i = 1$ та $p_1 = 6$, отримаємо:

$$\mathbf{M}_1 = \mathbf{M}_{PH} = \mathbf{PH} = \{\bigcup_{j=1}^{6} M_{1j}\} = \\ = \{M_{11}, M_{12}, M_{13}, M_{14}, M_{15}, M_{16}\} = \{C_5, I_4, A_3, A_2, P_1, U_0\}, \quad (6)$$

де $M_{11}=C_5$, $M_{12}=I_4$, $M_{13}=A_3$, $M_{14}=A_2$, $M_{15}=P_1$ та $M_{16}=U_0$ – характеристики, що використовуються в моделі Гексада Паркера – конфіденційність, цілісність, доступність, автентичність, керованість та практичність відповідно. Аналогічно, використовуючи послідовно (3) та (4) для Моделі STRIDE, наприклад, при $i=2$ та $p_2=6$, отримаємо:

$$\mathbf{M}_2=\mathbf{M}_{STRIDE}=\mathbf{STRIDE}=\{\bigcup_{j=1}^{6}M_{2j}\}=\{M_{21},M_{22},M_{23},M_{24},M_{25},M_{26}\}=\{S_5,T_4,R_3,I_2,D_1,E_0\}, \quad (7)$$

де $M_{21}=S_5$, $M_{22}=T_4$, $M_{23}=R_3$, $M_{24}=I_2$, $M_{25}=D_1$ та $M_{26}=E_0$ – характеристики, що використовуються в Моделі STRIDE – захищеність від підміни даних, зміни даних, відмови від відповідальності, розголошення інформації, відмови в обслуговуванні та захоплення привілеїв відповідно. Далі відповідно, використовуючи послідовно (3) та (4) для моделі 5A, наприклад, при $i=3$ та $p_3=5$, отримаємо:

$$\mathbf{M}_3=\mathbf{M}_{5A}=5\mathbf{A}=\{\bigcup_{j=1}^{5}M_{3j}\}=\{M_{31},M_{32},M_{33},M_{34},M_{35}\}=\{A_4,A_3,A_2,A_1,A_0\}, \quad (8)$$

де $M_{31}=A_4$, $M_{32}=A_3$, $M_{33}=A_2$, $M_{34}=A_1$ та $M_{35}=A_0$ – характеристики, що використовуються в Моделі 5A – аутентифікація, авторизація, доступність, автентичність та допустимість відповідно.

На основі табл. 1 і виразів (2), (3), та (4) сформуємо співвідношення вимог до режиму безпеки, на базі яких будується відповідна таблиця (табл. 3), де $\underset{j=1}{\overset{p_i}{\mathrm{CON}}}(M_{ij})$ $(j=\overline{p_i,1;-1})$ – операція конкатенації (склеювання об'єктів лінійної структури) $(M_{ij}=1)\vee(M_{ij}=0)$.

Таблиця 3

Забезпечення характеристик різних режимів безпеки (загальний вигляд)

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} (при $i=\overline{1,n}$, $j=\overline{1,m_i}$, n, m_i, r_{ij})	R_{ijk} *code*	Режим безпеки			
				$\mathbf{M}_1$	$\mathbf{M}_2$	…	$\mathbf{M}_q$
				$M_{11},M_{12},...,M_{1p_1}$	$M_{21},M_{22},...,M_{2p_2}$		$M_{q1},M_{q2},...,M_{qp_n}$
$\mathbf{R}_1$, … $\mathbf{R}_n$	$\mathbf{R}_{11}$, ... $\mathbf{R}_{nm_n}$	$R_{111}...R_{ijk}$ *description*	R_{111} ... $R_{nm_nr_{nm_n}}$	$\underset{j=1}{\overset{p_1}{\mathrm{CON}}}(M_{1j})$	$\underset{j=1}{\overset{p_2}{\mathrm{CON}}}(M_{2j})$	…	$\underset{j=1}{\overset{p_n}{\mathrm{CON}}}(M_{qp_n})$

У випадку якщо забезпечується ij-та характеристика i-ї МКБ, то $M_{ij}=1$, в іншому випадку – $M_{ij}=0$. Таким чином, з використанням зазначеної операції конкатенації, формуються бінарні послідовності, які характеризують режими безпеки згідно моделей $\mathbf{M}_i$.

Наприклад, якщо забезпечено вимогу VR_2 = «Засоби криптографічного захисту даних», то режими безпеки формуються таким чином:

– за моделлю **PH** режим безпеки **«110100»** $(C_5=1,\ I_4=1,\ A_3=0,\ A_2=1,\ P_1=0,\ U_0=0)$;

– за моделлю **STRIDE** режим безпеки **«111100»** $(S_5=1,\ T_4=1,\ R_3=1,\ I_2=1,\ D_1=0,\ E_0=0)$;

– за моделлю 5**A** режим безпеки **«10010»** $(A_4=1,\ A_3=0,\ A_2=0,\ A_1=1,\ A_0=0)$.

Таким чином, для ЦА України, враховуючи зазначені МКБ **PH**, **STRIDE** та 5**A**, а також (5), (6), (7) та (8), табл. 3 матиме вигляд, представлений у табл. 4.

Для зручності, аналогічно описаному в [15] підходу, представимо характеристики МКБ M_{ij} у шістнадцятковій системі числення (табл. 5) наступним чином:

$$(M_{11}M_{12}...M_{1p_1})_{(2)},(M_{21}M_{22}...M_{2p_2})_{(2)},...,(M_{q1},M_{q2},...,M_{qp_n})_{(2)}=SR_{1(16)},SR_{2(16)},...,SR_{q(16)}. \quad (9)$$

З урахуванням виразу (9) режим безпеки в результаті забезпечення вимоги R_{ijk} можна представити відповідно до i-ї МКБ або в мультирівневому представленні як $SR_{1(16)}:SR_{2(16)}:\ldots:SR_{q(16)}$.

Для прикладу, якщо забезпечено згадану вимогу VR_2 (виділено сірим кольором у табл. 4 та табл. 6), то режими безпеки формуються таким чином:

– за моделлю **PH** режим безпеки *«34»* $(110100_{(2)}=34_{(16)})$;

– за моделлю **STRIDE** режим безпеки *«3C»* $(111100_{(2)}=3C_{(16)})$;

– за моделлю 5**A** режим безпеки *«12»* $(10010_{(2)}=12_{(16)})$.

Таблиця 4

Забезпечення характеристик різних режимів безпеки

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} (при $m_1=4,\ r_{11}=5,\ r_{12}=4,\ r_{13}=7,\ r_{14}=6,\ m_2=1,\ r_{21}=13,\ m_3=2,\ r_{31}=5,\ r_{32}=4$)	R_{ijk} *code*	Режим безпеки		
				PH	**STRIDE**	**5A**
				$C_5I_4A_3A_2P_1U_0$	$S_5T_4R_3I_2D_1E_0$	$A_4A_3A_2A_1A_0$
$\mathbf{ICAO}_1$	**AR**	Стандарти, політика і процедури забезпечення безпеки	AR_1	000001	000000	00001
		Відбір, підготовка та перепідготовка персоналу	AR_2	000001	000000	00000
		Оцінка загроз та ризиків з метою визначення уразливостей КАІС і ймовірності атаки	AR_3	000001	000001	00001
		Контроль якості послуг, включаючи перевірки та інспекції	AR_4	000000	000000	00000
		Безпека ланцюга поставки ПЗ та обладнання	AR_5	000111	001000	00011
$\mathbf{ICAO}_2$	**VR**	Засоби мережевого захисту	VR_1	111000	110110	11100
		Засоби криптографічного захисту даних	VR_2	110100	111100	10010
		Системи виявлення / попередження вторгнень до КАІС	VR_3	001010	100010	01000
		Системи антивірусного захисту та протидії шкідливому ПЗ	VR_4	111100	111111	11111
$\mathbf{ICAO}_3$	**PC**	Захист обладнання та контроль доступу до нього	PC_1	001010	100011	01100
		Аутентифікація легітимних користувачів КАІС	PC_2	000100	001001	01000
		Обмеження кола осіб, що мають доступ до ресурсів КАІС	PC_3	001010	000011	00101
		Чітка пропускна система	PC_4	001110	000011	01101
		Постійний контроль та управління доступом до КАІС	PC_5	001010	000010	01100
		Використання автономних резервних систем	PC_6	011000	010010	00110
		Ведення журналів реєстрації операцій та експлуатаційних параметрів	PC_7	000100	111000	00001
$\mathbf{ICAO}_4$	**ATC**	Визначення переліку КАІС	ATC_1	000001	000000	00001
		Захист КАІС від НСД	ATC_2	110000	110101	10010
		Попередження вторгнень у роботу КАІС	ATC_3	001010	100010	01000
		Виявлення атак на КАІС	ATC_4	001010	100010	01000
		Застосування процедур оцінювання ризиків	ATC_5	000001	000001	00001
		Оцінювання уразливостей та наслідків відмов КАІС	ATC_6	000001	000001	00011
$\mathbf{ECAC}_1$	**SC**	Застосування заходів безпеки до КАІС	SC_1	111100	111111	11100
		Включення КАІС до процесу оцінки загроз	SC_2	000001	000001	00001
		Відділення КАІС від публічних мереж	SC_3	110010	111101	10111
		Мінімізація підключень до КАІС і контроль доступу	SC_4	001010	000011	00101
		Відбір, підготовка та перепідготовка операторів, що обслуговують КАІС	SC_5	000001	000000	00000
		Координація й узгодження заходів щодо захисту КАІС з існуючими заходами щодо авіаційної безпеки	SC_6	000001	000000	00000
		Врахування заходами захисту форми, впровадження, управління й застосування нових КАІС	SC_7	000001	000000	00000
		Використання заходів захисту прийнятного рівня в існуючих КАІС	SC_8	000011	000000	00000
		Забезпечення прийнятних заходів безпеки до апаратного та програмного забезпечення, що використовується в КАІС	SC_9	000011	000000	00000
		Безпека ланцюга поставки апаратних і програмних засобів КАІС	SC_{10}	000111	001000	00011
		Забезпечення віддаленого доступу до КАІС за узгоджених і безпечних умов	SC_{11}	001100	001010	11100
		Виключення можливості несанкціонованого доступу постачальників після купівлі КАІС	SC_{12}	000010	000001	01000
		Ведення обліку й оцінки кібератак на КАІС	SC_{13}	000001	000000	00011
$\mathbf{NATIONAL}_1$	**OR**	Визначення пріоритетів державної політики в сфері протидії КЗ у ЦА	OR_1	000000	000000	00000
		Державний нагляд за станом захисту КАІС від КЗ	OR_2	000000	000000	00000
		Включення КАІС до процесу оцінки загроз ЦА	OR_3	000001	000001	00001
		Ідентифікація КАІС, збір, узагальнення та облік даних	OR_4	001001	111000	00001
		Впровадження системи відбору, перевірки та підготовки фахівців з питань протидії КЗ у ЦА	OR_5	000001	000000	00000
$\mathbf{NATIONAL}_2$	**TR**	Визначення повного переліку КАІС	TR_1	000001	000000	00001
		Створення моделі загроз для кожної КАІС	TR_2	000001	000001	00001
		Реалізація технічного захисту КАІС	TR_3	100110	000100	11000
		Контроль за ефективністю заходів захисту	TR_4	000000	000000	00001

Таблиця 5

Шістнадцяткове кодування режимів безпеки (загальний вигляд)

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} *code*	Режим безпеки			
			$\mathbf{M}_1$	$\mathbf{M}_2$	…	$\mathbf{M}_q$
$\mathbf{R}_1$ … $\mathbf{R}_n$	$\mathbf{R}_{11}$ ... $\mathbf{R}_{nm_n}$	R_{111}. .. $R_{nm_n r_{nm_n}}$	$SR_{1(16)}$	$SR_{2(16)}$	…	$SR_{q(16)}$

Для ЦА України, враховуючи (9) табл. 5 трансформується у табл. 6.

Таблиця 6

Шістнадцяткове кодування режимів безпеки ЦА України

$\mathbf{R}_i$	$\mathbf{R}_{ij}$	R_{ijk} *code*	Режим безпеки		
			PH	**STRIDE**	**5A**
ICAO$_1$	**AR**	AR_1	01	00	01
		AR_2	01	00	00
		AR_3	01	01	01
		AR_4	00	00	00
		AR_5	07	08	03
ICAO$_2$	**VR**	VR_1	38	36	1C
		VR_2	34	3C	12
		VR_3	0A	22	08
		VR_4	3C	3F	1F
ICAO$_3$	**PC**	PC_1	0A	23	0C
		PC_2	04	09	08
		PC_3	0A	03	05
		PC_4	0E	03	0D
		PC_5	0A	02	0C
		PC_6	18	12	06
		PC_7	04	38	01
ICAO$_4$	**ATC**	ATC_1	01	00	01
		ATC_2	30	35	12
		ATC_3	0A	22	08
		ATC_4	0A	22	08
		ATC_5	01	01	01
		ATC_6	01	01	03
ECAC$_1$	**SC**	SC_1	3C	3F	1C
		SC_2	01	01	01
		SC_3	32	3D	17
		SC_4	0A	03	05
		SC_5	01	00	00
		SC_6	01	00	00
		SC_7	01	00	00
		SC_8	03	00	00
		SC_9	03	00	00
		SC_{10}	07	08	03
		SC_{11}	0C	0A	1C
		SC_{12}	02	01	08
		SC_{13}	01	00	03
NATIONAL$_1$	**OR**	OR_1	00	00	00
		OR_2	00	00	00
		OR_3	01	01	01
		OR_4	09	38	01
		OR_5	01	00	00
NATIONAL$_2$	**TR**	TR_1	01	00	01
		TR_2	01	01	01
		TR_3	26	04	18
		TR_4	00	00	01

У мультирівневому представленні в результаті виконання вимоги VR_2 буде забезпечено режим безпеки *34:3C:12* – це означає, що *забезпечення вимоги «Засоби криптографічного захисту даних», яка задекларована в керівному документі ICAO DOC 8973/8 у розділі 18.1.6.b «Віртуальне регулювання», дозволить забезпечити: конфіденційність, цілісність та автентичність за Гексадою Паркера; захищеність від підміни даних, зміни даних, відмови від відповідальності, розголошення інформації за моделлю STRIDE; аутентифікацію та автентичність за моделлю 5A.*

Висновки

Таким чином, у цій роботі розроблено мультирівневу модель, яка за рахунок використання базової моделі формування вимог до забезпечення КБ ЦА, конкатенації бінарних послідовностей, що характеризують режими безпеки, та бінарно-шістнадцяткового кодового представлення характеристик безпеки, множини МКБ та підмножин характеристик безпеки (розширених підмножин, що враховують додаткові характеристики безпеки), дозволяє формалізувати процес ідентифікації забезпеченості вимог та визначення режимів безпеки критичних авіаційних інформаційних систем. У подальших дослідженнях планується розробити метод оцінювання повноти забезпечення вимог у результаті реалізації відповідних методів та засобів захисту ЦА від кіберзагроз.

ЛІТЕРАТУРА

[1]. Зелена книга з питань захисту критичної інфраструктури в Україні. Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2014_table /1125_zelknuga.pdf.

[2]. Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, О.Г. Корченко, Ю.Б. Чеботаренко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). – К. : НАУ, 2009. – С. 131-140.

[3]. Гнатюк С.О. Сучасні критичні авіаційні інформаційні системи / С.О. Гнатюк, Д.В. Васильєв // Безпека інформації. – Т. 22, № 1. – 2016. – С. 51-57.

[4]. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. – Т. 19, № 2. – 2013. – С. 118-129.

[5]. Гнатюк С.О. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / С.О. Гнатюк, О.А. Шаховал, І.Л. Лозова // Захист інформації. – 2016. – Т. 18, №1. – С. 57-65.

[6]. Харченко В.П. Базова модель формування вимог до забезпечення кібербезпеки цивільної авіації / В.П. Харченко, О.Г. Корченко, С.О. Гнатюк // Безпека інформації. – 2016. – Т.22. – №2. – С. 150-155.

[7]. Doc 30 «Политика ЕКГА в сфере авиационной безопасности» (Restricted). – Изд. 13. – 2010. – 138 с.

[8]. Doc 8973 ICAO «Руководство по авиационной безопасности» (Restricted). – Изд. 8. – 2011. – 748 с.

[9]. Doc 9985 ICAO «Руководство по безопасности системы организации воздушного движения» (Restricted). – Изд. 1. – 2013. – 174 с.
[10]. Проект Закону України «Про Державну програму авіаційної безпеки цивільної авіації» [Електронний ресурс]. – Режим доступу: http://avia.gov.ua/uploads/documents/8774.pdf
[11]. Communication network dependencies for ICS/SCADA Systems, European Union Agency for Network and Information Security. – 2016. – 80 p.
[12]. Pender-Bey G. The Parkerian Hexad: The CIA Triad Model Expanded. – Available at: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.Pdf.
[13]. The STRIDE Threat Model. – Available at: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.
[14]. Updating the Traditional Security Model. – Available at: https://www.schneier.com/blog/archives/ 2006/08/updating_the_tr.html.
[15]. Корченко А.Г. Построение систем защиты информации на нечетких множествах: Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

REFERENCES

[1]. Green Paper on Critical Infrastructure Protection in Ukraine. National Institute of Strategic Studies. [Electronic resource] Access mode: http://www.niss.gov.ua/public/File/2014_table/1125_zelknuga.pdf.
[2]. Kharchenko V.P. Cyberterrorism in aviation transport / V.P. Kharchenko, O.G. Korchenko, Yu.B. Chebotarenko, E.V. Patsira, S.O. Gnatyuk // Proceedings "Problems of informatization and management". Vol. 4 (28)., K. : NAU, 2009, pp. 131-140.
[3]. Gnatyuk S.O. Modern critical aviation information systems / S.O. Gnatyuk, D.V. Vasiliev // Ukrainian scientific journal of information security, V. 22, № 1, 2016, pp. 51-57.
[4]. Gnatyuk S.O. Cyberterrorism: the history of development, modern trends and countermeasures / S.O. Gnatyuk // Ukrainian scientific journal of information security. V. 19, № 2, 2013, pp. 118-129.
[5]. Gnatyuk S.O. recommendations for cybersecurity strategy of Ukraine development/ S.O. Gnatyuk, O.A. Shahoval, I.L. Lozova // Ukrainian information security research journal. 2016. V. 18, №1, pp. 57-65.
[6]. Kharchenko V.P. The base model of cybersecurity requirements in civil aviation / V.P. Kharchenko, O.G. Korchenko, S.O. Gnatyuk // Ukrainian scientific journal of information security. 2016, V.22, №2, pp. 150-155.
[7]. Doc 30 «ECAC policy in the field of aviation security» (Restricted). Ed. 13, 2010, 138 p.
[8]. Doc 8973 ICAO «Aviation Security Guide» (Restricted). Ed. 8, 2011, 748 p.
[9]. Doc 9985 ICAO «Air traffic management system safety guide» (Restricted). Ed. 1, 2013, 174 p.
[10]. Draft Law of Ukraine "About the Government program of the aviation safety services of civil aviation" [Electronic resource] Access mode: http://avia.gov.ua/ uploads/documents/8774.pdf.
[11]. Communication network dependencies for ICS/SCADA Systems, European Union Agency for Network and Information Security. – 2016. – 80 p.
[12]. Pender-Bey G. The Parkerian Hexad: The CIA Triad Model Expanded. – Available at: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf
[13]. The STRIDE Threat Model. – Available at: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.
[14]. Updating the Traditional Security Model. – Available at: https://www.schneier.com/blog/archives/ 2006/08/updating_the_tr.html.
[15]. Korchenko A.G. Construction of information security systems on fuzzy sets: theory and practical solutions / A.G. Korchenko. K., MK-press, 2006, 320 p.

МУЛЬТИУРОВНЕВАЯ МОДЕЛЬ ДАННЫХ ДЛЯ ИДЕНТИФИКАЦИИ ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЙ СОГЛАСНО НОРМАТИВНО-ПРАВОВОМУ ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКОЙ АВИАЦИИ

Сегодня защита критической инфраструктуры является одной из первоочередных задач государства, особенно остро этот вопрос встает перед государствами, внедряющих новейшие информационно-коммуникационные технологии во всех критических областях. Указанные технологии, помимо прочего, порождают целый ряд новых уязвимостей и потенциальных киберугроз. В области гражданской авиации уровень критичности значительно усиливается коммуникацией и взаимодействием между наземными системами и воздушными судами. Известная модель формирования требований к обеспечению кибербезопасности гражданской авиации позволяет формализовать процесс создания полного множества требований, которые необходимо обеспечить для защиты гражданской авиации от киберугроз, однако отсутствует механизм определения обеспеченности режимов безопасности вследствие реализации методов и средств, задекларированных в соответствующих требованиях. Учитывая это, актуальной является разработка подхода к определению обеспеченности режимов безопасности, что учитывает дополнительные характеристики безопасности. В этой работе предложено мультиуровневая модель данных которая, за счет использования базовой модели формирования требований к обеспечению кибербезопасности гражданской авиации, конкатенации бинарных последовательностей, которые характеризуют режимы безопасности, и бинарно-шестнадцате-

ричного кодового представления характеристик безопасности, множества моделей безопасности и подмножеств характеристик безопасности (с учетом дополнительных), позволяет формализовать процесс идентификации обеспеченности требований и определения режимов безопасности критических авиационных информационных систем. В дальнейших исследованиях планируется разработать метод оценки полноты обеспечения требований в результате реализации соответствующих методов и средств защиты.

Ключевые слова: кибербезопасность, гражданская авиация, критическая информационная авиационная система, модель идентификации, нормативно-правовое обеспечение, модель безопасности, характеристика безопасности.

MULTILEVEL DATA MODEL FOR REQUIREMENTS PROVIDING IDENTIFICATION ACCORDINGLY TO REGULATORY SUPPORT FOR CIVIL AVIATION CYBERSECURITY

Critical infrastructure protection is one of the priorities for states. Particularly acute issue appears to states implementing new information and communication technologies in all critical areas. These technologies, among other things, generate a number of new vulnerabilities and potential cyberthreats. In the civil aviation criticality level substantially reinforced by communication and interaction between ground and aircraft systems. Well-known model of cybersecurity requirements in civil aviation allows to formalize the process of complete set of requirements creating that are necessary to ensure civil aviation security against cyberthreats. But there is no mechanism for determining the availability of certain modes of security because of the methods and tools declared in the request. With this in mind, is to develop relevant approach to defining security regimes that takes account of additional security features. In this paper a multilevel model database was proposed, which through the use of a basic model of requirements to ensure cybersecurity of civil aviation concatenation of binary sequences that characterize the security mode and binary-hexadecimal coded representation of performance security set security models and subsets of performance security (with the additional features), allows to formalize the process of security requirements identification and determine the mode of critical aviation information systems security. In further research the development of method for evaluating the completeness of compliance is planned as a result of appropriate security methods and means implementation.

Index words: cybersecurity, civil aviation, critical aviation information system, identification model, regulatory support, security model, security features.

Харченко Володимир Петрович, доктор технічних наук, професор, проректор з наукової роботи Національного авіаційного університету.
E-mail: kharch@nau.edu.ua
Харченко Владимир Петрович, доктор технических наук, профессор, проректор по научной работе Национального авиационного университета.
Kharchenko Volodymyr, Dr Eng, Professor, Vice-Rector for Scientific Research in National Aviation University.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, визит-профессор Университета в Бельско-Бялой (Гуманитарно-техническая академия в Бельско-Бялой, г. Бельско-Бяла, Польша), ведущий научный сотрудник Национальной академии СБ Украины.
E-mail: icaocentre@nau.edu.ua
Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, візит-професор Університету в Бельсько-Бялій (Гуманітарно-технічна академія в Бельсько-Бялій, м. Бельсько-Бяла, Польща), провідний науковий співробітник Національної академії СБ України.
Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Humanistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
Гнатюк Сергей Александрович, кандитат технических наук, доцент, доцент кафедры информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-Security Academic Dept in National Aviation University.