

БАЗОВА МОДЕЛЬ ФОРМУВАННЯ ВИМОГ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

Володимир Харченко, Олександр Корченко, Сергій Гнатюк

Національний авіаційний університет, Україна



ХАРЧЕНКО Володимир Петрович, д.т.н.

Рік і місце народження: 1943 рік, м. Оратів, Вінницька область, Україна.

Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет), 1967 рік.

Посада: проректор з наукової роботи з 2001 року, виконуючий обов'язки ректора з 2015 року.

Наукові інтереси: інформаційні технології аерокосмічних систем навігаційного обслуговування польотів на основі супутникових систем CNS/ATM, безпека безпілотних авіаційних систем.

Публікації: понад 500 наукових робіт, включаючи монографії, підручники, навчальні посібники, статті, патенти, які опубліковано як в Україні, так і за кордоном.

E-mail: kharch@nau.edu.ua



КОРЧЕНКО Олександр Григорович, д.т.н.

Рік і місце народження: 1961 рік, м. Київ, Україна.

Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет), 1983 рік.

Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.

Наукові інтереси: інформаційна та авіаційна безпека.

Публікації: більше 300 наукових публікацій, серед яких монографії, словники, навчальні посібники, підручники, наукові статті, патенти та авторські свідоцтва на винаходи.

E-mail: agkorchenko@gmail.com



ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.

Освіта: Національний авіаційний університет, 2007 рік.

Посада: доцент кафедри безпеки інформаційних технологій з 2012 року, голова Наукового товариства студентів, аспірантів, докторантів та молодих вчених з 2015 року.

Наукові інтереси: інформаційна безпека, квантова криптографія, управління інцидентами інформаційної безпеки, захист критичної інформаційної інфраструктури держави.

Публікації: більше 200 наукових публікацій, серед яких монографії, статті у рецензованих вітчизняних та закордонних наукових журналах, патенти та авторські свідоцтва.

E-mail: s.gnatyuk@nau.edu.ua

Анотація. Проблема кібертероризму носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Провідні держави світу все більше уваги приділяють кіберзахисту власних критичних інфраструктур. У галузі цивільної авіації рівень критичності значно підвищується підвищенням ступенем комунікації та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій з одного боку підвищує ефективність діяльності цивільної авіації, а з іншого – породжує цілу низку нових уразливостей та потенційних загроз. Існуючі розробки не в повній мірі враховують сучасні вимоги, задекларовані в керівних документах щодо безпеки авіації, та специфіку діяльності цивільної авіації. Виходячи з цього, на базі керівних документів щодо безпеки міжнародної цивільної авіації, запропонована базова модель формування вимог до забезпечення кібербезпеки авіаційної галузі. Крім того, формалізовано вітчизняні вимоги щодо забезпечення кібербезпеки цивільної авіації, що дозволить сформувати відповідну державну авіаційну систему кібербезпеки України. У подальших роботах планується розробка ефективних методів та засобів щодо забезпечення сформованих у цій роботі вимог.

Ключові слова: кібербезпека, цивільна авіація, критична інформаційна авіаційна система, кіберзагрози, формування вимог, керівний документ, базова модель, ІКАО, ЄКЦА.

Вступ

Проблема кібертероризму [1] носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Провідні держави світу

все більше уваги приділяють кіберзахисту власних критичних інфраструктур. Одним з важливих об'єктів критичної інфраструктури є транспортна система (поряд, наприклад, з енергетичною, нафто-

ва газотранспортною системами), несанкціоноване втручання у роботу якої може призвести до значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури. Особливої уваги заслуговує цивільна авіація (ЦА) [2], рівень критичності якої значно підвищується підвищеним ступенем комунікації та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій (КТ) з одного боку підвищує ефективність і спрощує формальності у діяльності ЦА, а з іншого – породжує цілу низку нових уразливостей та потенційних загроз. Стандарт ІКАО [3] декларує необхідність для кожної держави, яка є членом ІКАО, розробляти методи захисту ІКТ, що використовуються для цілей ЦА, від актів незаконного втручання, які можуть поставити під загрозу безпеку міжнародної ЦА. Керівний документ Європейської конференції ЦА (ЕСАС) [4] визначає необхідність включення заходів щодо забезпечення захисту відповідної галузі від кіберзагроз (КЗ) до національної програми безпеки ЦА та інших національних програм (контролю якості, навчання і підготовки персоналу з питань безпеки ЦА тощо). Відповідно до [3-4] обов'язково необхідно ідентифікувати та захищати системи, які містять інформацію, що має критичне значення для безпечного виконання польотів і безпечної діяльності ЦА – це так звані критичні авіаційні інформаційні системи (КАІС) [5], орієнтовний перелік яких наведено у відповідному керівному документі [6]. Несанкціонований доступ (НСД) і використання КАІС може призвести до виникнення загроз безпеці пасажирів, екіпажу та наземного персоналу, з огляду на що важливим є забезпечення їх кібербезпеки (КБ) шляхом захисту від НСД, попередження втручання у роботу КАІС та виявлення атак на них.

Аналіз існуючих досліджень і постановка завдання

Серед робіт, пов'язаних із забезпеченням КБ транспорту, варто виділити праці В. Лакна [7-10], які спрямовані на підвищення безпеки інформаційно-комунікаційного середовища транспорту шляхом розробки моделей та методів захисту інформації на основі інтелектуального розпізнавання загроз в умовах збільшення кількості дестабілізуючих впливів на об'єкти критичної інфраструктури держави; Г. Вільського [11-12], що орієнтовані на забезпечення інформаційної безпеки судноплавства.

У галузі ЦА варто виділити праці Р. Акіншина [13-14], які націлені на підвищення інформаційної безпеки автоматизованих систем

$$\mathbf{R} = \left\{ \bigcup_{i=1}^n \mathbf{R}_i \right\} = \left\{ \bigcup_{i=1}^n \left\{ \bigcup_{j=1}^{m_i} \mathbf{R}_{ij} \right\} \right\} = \left\{ \{ \mathbf{R}_{11}, \mathbf{R}_{12}, \dots, \mathbf{R}_{1m_1} \}, \{ \mathbf{R}_{21}, \mathbf{R}_{22}, \dots, \mathbf{R}_{2m_2} \}, \dots, \{ \mathbf{R}_{n1}, \mathbf{R}_{n2}, \dots, \mathbf{R}_{nm_n} \} \right\}, (i = \overline{1, n}, j = \overline{1, m_i}). \quad (3)$$

Множини наборів вимог $\mathbf{R}_{ij} \subseteq \mathbf{R}_i$ визначимо таким чином:

$$\mathbf{R}_{ij} = \left\{ \bigcup_{k=1}^{r_{ij}} R_{ijk} \right\} = \left\{ R_{ij1}, R_{ij2}, \dots, R_{ijr_{ij}} \right\}, \quad (4)$$

збору, обробки, зберігання та поширення даних, що забезпечують аеронавігаційні системи і користувачів повітряного простору аеронавігаційною інформацією в умовах збільшення інтенсивності польотів; А. Міщенко [15-16], що пов'язані з управлінням інформаційною безпекою авіатранспортного комплексу за рахунок розробки методологічного та організаційно-технічного забезпечення низки етапів циклу РДСА.

Проте, більшість відомих робіт орієнтована на розробку або загальних підходів до забезпечення КБ, або створення методів, моделей та засобів щодо забезпечення конфіденційності, цілісності й доступності інформації, що обробляється, зберігається чи передається за допомогою сучасних ІКТ. Таким чином, відповідно до поточного стану досліджень, не в повній мірі враховуються сучасні вимоги, задекларовані в керівних документах щодо безпеки авіації, та специфіка діяльності ЦА. З огляду на це, метою роботи є розробка базової моделі формування вимог до забезпечення КБ ЦА на базі керівних документів, пов'язаних з безпекою міжнародної ЦА.

Основна частина дослідження

Для формування державної системи КБ у галузі ЦА необхідно забезпечити виконання низки вимог, які містяться у різних керівних документах щодо безпеки ЦА (стандартах, рекомендованих практиках та національних програмах). Для розробки базової моделі формування вимог, відповідно до наведеного в [17] підходу, введемо відповідну базову множину всіх вимог \mathbf{R} :

$$\mathbf{R} = \left\{ \bigcup_{i=1}^n \mathbf{R}_i \right\} = \{ \mathbf{R}_1, \mathbf{R}_2, \dots, \mathbf{R}_n \}, \quad (1)$$

де $\mathbf{R}_i \subseteq \mathbf{R}$ ($i = \overline{1, n}$) – множини наборів вимог відповідних керівних органів, n – загальна кількість вимог відповідних керівних органів, а

$$\mathbf{R}_i = \left\{ \bigcup_{j=1}^{m_i} \mathbf{R}_{ij} \right\} = \{ \mathbf{R}_{i1}, \mathbf{R}_{i2}, \dots, \mathbf{R}_{im_i} \}, \quad (2)$$

при чому \mathbf{R}_{ij} ($i = \overline{1, n}, j = \overline{1, m_i}$) – множини наборів вимог i -го керівного органу; m_i – кількість вимог i -го керівного органу.

З урахуванням (2) вираз (1) можна представити у наступному вигляді:

де R_{ijk} ($i = \overline{1, n}, j = \overline{1, m_i}, k = \overline{1, r_{ij}}$) – вимоги з множини набору вимог \mathbf{R}_{ij} , r_{ij} – кількість таких вимог у кожній з множин ij -го набору.

Тоді вираз (3) з урахуванням (4) матиме такий вигляд:

$$\begin{aligned}
 \mathbf{R} &= \left\{ \bigcup_{i=1}^n \mathbf{R}_i \right\} = \left\{ \bigcup_{i=1}^n \left\{ \bigcup_{j=1}^{m_i} \mathbf{R}_{ij} \right\} \right\} = \left\{ \bigcup_{i=1}^n \left\{ \bigcup_{j=1}^{m_i} \left\{ \bigcup_{k=1}^{r_{ij}} \mathbf{R}_{ijk} \right\} \right\} \right\} = \\
 &= \{ \{ \{ R_{111}, R_{112}, \dots, R_{11r_{11}} \}, \{ R_{121}, R_{122}, \dots, R_{12r_{12}} \}, \dots, \{ R_{1m_1 1}, R_{1m_1 2}, \dots, R_{1m_1 r_{m_1}} \} \}, \\
 &\{ \{ R_{211}, R_{212}, \dots, R_{21r_{21}} \}, \{ R_{221}, R_{222}, \dots, R_{22r_{22}} \}, \dots, \{ R_{2m_2 1}, R_{2m_2 2}, \dots, R_{2m_2 r_{m_2}} \} \}, \dots, \\
 &\{ \{ R_{n11}, R_{n12}, \dots, R_{n1r_{n1}} \}, \{ R_{n21}, R_{n22}, \dots, R_{n2r_{n2}} \}, \dots, \{ R_{nm_n 1}, R_{nm_n 2}, \dots, R_{nm_n r_{m_n}} \} \} \}.
 \end{aligned} \tag{5}$$

Розглянемо приклад формування вимог щодо забезпечення КБ ЦА України. У цьому випадку, наприклад, при $n = 3$ згідно виразу (1), можна сформулювати базову множину вимог \mathbf{R} , яка, з урахуван-

$$\mathbf{R} = \mathbf{R}_{civil_aviation} = \left\{ \bigcup_{i=1}^3 \mathbf{R}_i \right\} = \{ \mathbf{R}_1, \mathbf{R}_2, \mathbf{R}_3 \} = \{ \mathbf{R}_{ICAO}, \mathbf{R}_{ECAC}, \mathbf{R}_{NATIONAL} \} = \{ \mathbf{ICAO}, \mathbf{ECAC}, \mathbf{NATIONAL} \},$$

де $\mathbf{R}_1 = \mathbf{R}_{ICAO} = \mathbf{ICAO}$, $\mathbf{R}_2 = \mathbf{R}_{ECAC} = \mathbf{ECAC}$ та $\mathbf{R}_3 = \mathbf{R}_{NATIONAL} = \mathbf{NATIONAL}$ - множини вимог ICAO, ECAC та національних відповідно.

ням відповідної існуючої нормативно-правової національної та міжнародної бази, складається з трьох множин:

Далі, використовуючи послідовно вирази (2), (3), (4) та (5), на основі керівних документів [6, 18] (див. табл. 1), наприклад, при $i = 1$ та $m_1 = 4$, отримаємо:

$$\begin{aligned}
 \mathbf{R}_1 &= \mathbf{ICAO} = \left\{ \bigcup_{j=1}^4 \mathbf{R}_{1j} \right\} = \{ \mathbf{R}_{11}, \mathbf{R}_{12}, \mathbf{R}_{13}, \mathbf{R}_{14} \} = \{ \mathbf{R}_{ICAO_1}, \mathbf{R}_{ICAO_2}, \mathbf{R}_{ICAO_3}, \mathbf{R}_{ICAO_4} \} = \\
 &= \{ \mathbf{ICAO}_1, \mathbf{ICAO}_2, \mathbf{ICAO}_3, \mathbf{ICAO}_4 \} = \{ \mathbf{AR}, \mathbf{VR}, \mathbf{PC}, \mathbf{ATC} \} = \\
 &= \{ \{ AR_1, AR_2, \dots, AR_5 \}, \{ VR_1, VR_2, \dots, VR_4 \}, \{ PC_1, PC_2, \dots, PC_7 \}, \{ ATC_1, ATC_2, \dots, ATC_6 \} \},
 \end{aligned}$$

де $\mathbf{R}_{11} = \mathbf{R}_{ICAO_1} = \mathbf{ICAO}_1 = \mathbf{AR} = \{ AR_1, AR_2, \dots, AR_5 \}$,
 $\mathbf{R}_{12} = \mathbf{R}_{ICAO_2} = \mathbf{ICAO}_2 = \mathbf{VR} = \{ VR_1, VR_2, \dots, VR_4 \}$ та
 $\mathbf{R}_{13} = \mathbf{R}_{ICAO_3} = \mathbf{ICAO}_3 = \mathbf{PC} = \{ PC_1, PC_2, \dots, PC_7 \}$ - відповідно множини вимог адміністративного регулювання, віртуального регулювання та фізичного

контролю, сформованих на базі вимог, які містяться в п. 18.1.6 [6], а $\mathbf{R}_{14} = \mathbf{R}_{ICAO_4} = \mathbf{ICAO}_4 = \mathbf{ATC} = \{ ATC_1, ATC_2, \dots, ATC_6 \}$ - множина вимог контролю повітряного руху, сформована на базі вимог, які містяться в додатку В документу [18] (див. табл. 1).

Вимоги ICAO щодо захисту ЦА від КЗ

Таблиця 1

Елемент множини	Множина вимог	Елементи множини (при $i = 1, m_1 = 4, r_{11} = 5, r_{12} = 4, r_{13} = 7, r_{14} = 6$)	Ст. в [6,18]	Член множини
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 поставок 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 програмному забезпеченню	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 В Контроль повітряного руху (ATC)	Визначення переліку КАІС	Дод.В.3.2	ATC ₁
		Захист КАІС від НСД	Дод.В.3.3	ATC ₂
		Попередження вторгнень у роботу КАІС	Дод.В.3.3	ATC ₃
		Виявлення атак на КАІС	Дод.В.3.3	ATC ₄
		Застосування процедур оцінювання ризиків	Дод.В.3.5	ATC ₅
		Оцінювання уразливостей та наслідків відмов КАІС	Дод.В.3.6	ATC ₆

Аналогічно, послідовно використовуючи вирази (2), (3), (4) та (5), на основі керівного документу

[4] (див. табл. 2), наприклад, при $i = 2$ та $m_2 = 1$, отримаємо:

$$\mathbf{R}_2 = \mathbf{ECAC} = \left\{ \bigcup_{j=1}^1 \mathbf{R}_{ij} \right\} = \{ \mathbf{R}_{21} \} = \{ \mathbf{R}_{ECAC_1} \} = \{ \mathbf{ECAC}_1 \} = \{ \mathbf{SC} \} = \{ SC_1, SC_2, \dots, SC_{13} \},$$

де $\mathbf{R}_{21} = \mathbf{R}_{ECAC_1} = \{ \mathbf{ECAC}_1 \} = \{ \mathbf{SC} \} = \{ SC_1, SC_2, \dots, SC_{13} \}$
 - множина вимог контролю на безпеку, сформова-

них на базі вимог, які містяться в пп. 1.1-1.8 розділу 14 документу [4] (див. табл. 2).

Вимоги ECAC щодо захисту ЦА від КЗ

Таблиця 2

Елемент множини	Множина вимог	Елементи множини (при $i = 2, m_2 = 1, r_{21} = 13$)	Ст. в [4]	Член множини
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 прийняттого 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

Далі відповідно, послідовно використовуючи вирази (2), (3), (4) та (5), на основі докуме-

нту [19] (див. табл. 3), при $i = 3$ та $m_3 = 2$ отримаємо:

$$\mathbf{R}_3 = \mathbf{NATIONAL} = \left\{ \bigcup_{j=1}^2 \mathbf{R}_{ij} \right\} = \{ \mathbf{R}_{31}, \mathbf{R}_{32} \} = \{ \mathbf{R}_{NATIONAL_1}, \mathbf{R}_{NATIONAL_2} \} = \{ \mathbf{NATIONAL}_1, \mathbf{NATIONAL}_2 \} = \{ \mathbf{OR}, \mathbf{TR} \} = \\ = \{ \{ OR_1, OR_2, \dots, OR_5 \}, \{ TR_1, TR_2, \dots, TR_4 \} \},$$

де $\mathbf{R}_{31} = \mathbf{R}_{NATIONAL_1} = \mathbf{NATIONAL}_1 = \mathbf{OR} = \{ OR_1, OR_2, \dots, OR_5 \}$ та $\mathbf{R}_{32} = \mathbf{R}_{NATIONAL_2} = \mathbf{NATIONAL}_2 = \mathbf{TR} = \{ TR_1, TR_2, \dots, TR_4 \}$ - відповідно

множини організаційних та технічних вимог, сформованих на базі ст. 174 та 175 документу [19] відповідно (див. табл. 2).

Вітчизняні вимоги щодо захисту ЦА від КЗ

Таблиця 3

Елемент множини	Множина вимог	Елементи множини (при $i = 3, m_3 = 2, r_{31} = 5, r_{32} = 4$)	Ст. в [19]	Член множини
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

Таким чином, відповідно до наведеного прикладу, для множини вимог щодо забезпечення КБ ЦА України $\mathbf{R} = \mathbf{R}_{civil_aviation}$, використовуючи вирази (3-5), 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:

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

де $R_{111} = R_{ICAO_{11}} = AR_1$, $R_{112} = R_{ICAO_{12}} = AR_2, \dots, R_{115} = R_{ICAO_{15}} = AR_5$, $R_{121} = R_{ICAO_{21}} = VR_1$, $R_{122} = R_{ICAO_{22}} = VR_2, \dots, R_{124} = R_{ICAO_{24}} = VR_4$, $R_{131} = R_{ICAO_{31}} = PC_1$, $R_{132} = R_{ICAO_{32}} = PC_2, \dots, R_{137} = R_{ICAO_{37}} = PC_7$, $R_{141} = R_{ICAO_{41}} = ATC_1$, $R_{142} = R_{ICAO_{42}} = ATC_2, \dots, R_{146} = R_{ICAO_{46}} = ATC_6$, $R_{211} = R_{ECAC_{11}} = SC_1$, $R_{212} = R_{ECAC_{12}} = SC_2, \dots, R_{21,13} = R_{ECAC_{1,13}} = SC_{13}$, $R_{311} = R_{NATIONAL_{11}} = OR_1$, $R_{312} = R_{NATIONAL_{12}} = OR_2, \dots, R_{315} = R_{NATIONAL_{15}} = OR_5$, $R_{321} = R_{NATIONAL_{21}} = TR_1$, $R_{322} = R_{NATIONAL_{22}} = TR_2, \dots, R_{324} = R_{NATIONAL_{24}} = TR_4$ - елементи відповідної базової множини, які відображають вимоги щодо забезпечення КБ ЦА України на базі [4, 6, 18, 19]; * - у випадку, якщо індекс є двозначним числом, то він відділяється комою

Висновки

Таким чином, у цій роботі запропоновано базову модель формування вимог до забезпечення кібербезпеки цивільної авіації, яка за рахунок введення базової множини вимог, які містяться у різних керівних документах щодо безпеки ЦА, та відповідних множин, що характеризують базову множину (множини наборів вимог відповідних керівних органів, множини наборів вимог i -го керівного органу), дає можливість формалізувати повну множину вимог, які необхідно забезпечити для захисту ЦА від КЗ, а також оцінити повноту забезпечення цих вимог.

Крім того, формалізовано вітчизняні вимоги щодо забезпечення КБ ЦА, забезпечення яких дозволить сформувати державну систему КБ України в галузі ЦА. У подальших роботах планується розробка ефективних методів та засобів для забезпечення сформованих у цій роботі вимог.

Література

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

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

[3] Приложение 17 к Конвенции о международной гражданской авиации «Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». - Изд. 9. - 2011. - 60 с.

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

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

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

[7] Лахно В. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту / В. Лахно // Безпека інформації. - 2016. - Т. 22, № 1. - С. 44-50.

[8] Лахно В. Інформаційна безпека інтелектуальних транспортних систем / В. Лахно // Захист інформації. - 2015. - Т. 17, № 4. - С. 298-305.

[9] Petrov O., Korchenko O., Lakhno V. Method and model of intellectual threats detection for information and communication transport environment // Ukrainian Scientific Journal of Information Security. - 2015. - Vol. 21, Issue 1. - P. 26-34.

[10] Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок: Монография / В.А. Лахно, А.С. Петров. - Луганск: изд-во ВНУ им. В. Даля, 2010. - 280 с.

[11] Вильский Г. Кластерно-вероятностная методология исследования информационной безопасности движения морских судов / Г. Вильский // Безпека інформації. - 2014. - Т. 20, № 1. - С. 92-96.

[12] Вильский Г. Удосконалення інформаційної безпеки субстандартного судноплавства / Г. Вильский, А. Бень // Безпека інформації. - 2015. - Т. 21, № 3. - С. 309-313.

[13] Модели для аналитической информационной системы поддержки принятия решений в

АСУ ПВО / Р.Н. Акиншин, В.П. Антонов, С.И. Анохин // Известия Тульского государственного университета. Серия: Проблемы специального машиностроения. – 2005. – С. 85-87.

[14] Автоматизированная обработка сигналов в реальном масштабе времени в автоматизированной системе УВД / Р.Н. Акиншин, Р.П. Быстров // Известия Тульского ГУ. Серия: Радиотехника и радиооптика. – 2006. – Т. 8, № 1. – С. 71-74.

[15] Міщенко А.В. Питання інформаційної безпеки в аспекті підвищення цільової ефективності авіатранспортного комплексу / А.В. Міщенко // Вісник Чернігівського держ. технолог. університету. Серія : Технічні науки. – 2015. – № 1. – С. 47-51.

[16] Міщенко А.В. Ресурсна оптимізація циклічних процесів лінійного типу функціонування авіатранспортного комплексу / А.В. Міщенко // Наукоємні технології. – 2014. – № 2. – С. 116-118.

[17] Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.

[18] Doc 9985 ICAO «Руководство по безопасности системы организации воздушного движения» (Restricted). – Изд. 1. – 2013. – 174 с.

[19] Проект Закона України «Про Державну програму авіаційної безпеки цивільної авіації» [Електронний ресурс]. – Режим доступу: <http://avia.gov.ua/uploads/documents/8774.pdf>.

УДК 004.056.5:343.326 (045)

Харченко В.П., Корченко А.Г., Гнатюк С.А. Базовая модель формирования требований к обеспечению кибербезопасности гражданской авиации

Аннотация. Проблема кибертерроризма носит глобальный характер и довольно остро стоит в современном информационном обществе. Ведущие государства мира все большее внимание уделяют киберзащите собственных критических инфраструктур. В области гражданской авиации уровень критичности значительно усиливается повышенной степенью коммуникации и взаимодействия между наземными системами и воздушными судами, а внедрение современных информационных и коммуникационных технологий с одной стороны повышает эффективность деятельности гражданской авиации, а с другой – порождает целый ряд новых уязвимостей и потенциальных угроз. Существующие разработки не в полной мере учитывают современные требования, задекларированные в руководящих документах по безопасности авиации, и специфику деятельности гражданской авиации. Исходя из этого, на базе руководящих документов по безопасности международной гражданской авиации, предложена базовая модель формирования требований по обеспечению кибербезопасности авиационной отрасли. Кроме того, формализованы отечественные требования по обеспечению кибербезопасности гражданской авиации, что позволит сформировать соответствующую государственную авиационную систему кибербезопасности Украины. В дальнейших работах планируется разработка эффективных методов и средств по обеспечению сформированных в этой работе требований.

Ключевые слова: кибербезопасность, гражданская авиация, критическая информационная авиационная система, киберугрозы, формирование требований, базовая модель, ИКАО, ЕКГА.

Kharchenko V., Korchenko O., Gnatyuk S. Basic model for cybersecurity requirements definition in civil aviation

Abstract. The problem of cyberterrorism is global and quite acute in today's information society. Leading world states are increasingly focused on critical infrastructures. In civil aviation criticality level is amplified by communication and interaction between ground systems and aircrafts. Modern information and communication technology implementation in one hand increases civil aviation operation efficiency and in the other hand generates a set of new vulnerabilities and potential threats. Existed solutions don't take into account modern requirements from regulatory aviation security documents in full and civil aviation specific. Accordingly, basic model for cybersecurity requirements definition based on regulatory international aviation security documents were proposed. Besides, domestic requirements for civil aviation cybersecurity were formalized and it allows to provide state aviation cybersecurity system of Ukraine. Further papers will relate to effective methods and means development for providing requirements formed in this paper.

Key words: cybersecurity, civil aviation, critical aviation information system, cyberthreats, requirements definition, basic model, ICAO, ECAS.

Отримано 12 травня 2016 року, затверджено редколегією 31 травня 2016 року