УДК 004.056.5::629.7.08 (045) **doi: 10.20998/2522-9052.2019.2.16**

В. М. Сидоренко, Ю. Я. Поліщук, С. О. Гнатюк

Національний авіаційний університет, Київ, Україна

ФОРМУВАННЯ ПЕРЕЛІКУ КРИТИЧНИХ АВІАЦІЙНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ РЕАЛІЗАЦІЇ КІБЕРЗАГРОЗ

Анотація. Предмет статті – методи, моделі та методики формування переліку об'єктів критичної інформаційної інфраструктури (КІІ). **Мета даної статті** – на основі розробленої уніфікованої моделі даних сформувати перелік критичних авіаційних інформаційних систем (КАІС) і визначити їх метрики зв'язності та складності. **Результати.** На основі раніше розробленої авторами уніфікованої моделі даних було створено методику формування переліку об'єктів КІІ, яка за рахунок мультирівневої деталізації, ієрархічного представлення множин, що характеризують системи та їх компоненти, а також введення матриці інцидентності кібербезпеки КІІ, її симплексних комплексів та Q-аналізу, дозволила сформулювати перелік КАІС та визначити їх зв'язність (співвідношення *q*-зв'язків множин кіберзагроз (КЗ) та КАІС). **Висновки.** Проведене дослідження показало, що відношення *q*- зв'язків множин КЗ має більш високу зв'язність у порівнянні з аналогічними відношеннями *q*-зв'язків множин систем КАІС, а це свідчить що реалізації однієї КЗ може ініціювати каскадний ефект на інші зв'язані загрози та призвести до важких, а іноді і руйнівних наслідків для певної системи КАІС. Крім того, обчислені міри складності комплексів $\varphi_{KAIS} = 1{,}39$ та $\varphi_{THREATS} = 1{,}13$ свідчать про більшу «складність» систем КАІС. Зазначені результати можуть бути використані відповідними державними органами для формування переліку об'єктів КІІ з метою застосування адекватних методів і засобів захисту.

Ключові слова: критична інфраструктура; критична інформаційна інфраструктура; критичні авіаційні інформаційні системи; кіберзагрози; симплекси; матриця інцидентності.

Вступ

Сучасні тенденції розвитку інформаційно-комунікаційних технологій (ІКТ) спричинили феноменальну залежність суспільства від послуг, які надають різноманітні галузі інфраструктури. Сьогодні якість та доступність таких послуг є одними з головних показників розвитку інфраструктури держави, а забезпечення їх захисту та стабільного функціонування є найважливішою і обов'язковою складовою національної безпеки розвинених держав. Збільшення концентрації засобів та ресурсів для захисту електронних інфраструктур різних типів зумовило необхідність ранжування інфраструктурних об'єктів, виділення найважливіших з них та появи поняття критична інфраструктура (КІ) держави. Зазвичай, до цієї категорії відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення мегаполісів, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Особливої уваги потребує авіаційна галузь, з огляду на необхідність забезпечення безперервної комунікації та взаємодії між наземними системами і повітряними суднами. Тому, першочерговим аспектом стає визначення об'єктів, які є критичними для забезпечення їх постійного функціонування. Проте, необмежена кількість об'єктів і параметрів систем, які постійно варіюються, та важко прогнозована поведінка об'єктів з великою кількістю взаємозв'язків є основними причинами труднощів виявлення об'єктів КІ держави.

1. Аналіз існуючих досліджень

Базовим компонентом КІ є інформаційна складова – критична інформаційна інфраструктура (КІІ). Основними причинами важливості КІІ є широке застосування ІКТ у всіх сферах людської діяльності, залежність від них громадян, суспільства і держави, а також збільшення уразливостей та потенційних загроз різного характеру. Крім того, в деяких державах особливий акцент ставиться на значення КІ для нації, навіть саме визначення КІІ вживається як критична національна інформаційна інфраструктура.

Аналіз вітчизняної нормативної бази свідчить, що галузь захисту КІІ у нашій державі перебуває на початковому етапі формування. Чинним законодавством досі не визначений вичерпний перелік об'єктів КІІ держави, а вказані лиш об'єкти окремих галузей [1–3], що потребують захисту з боку держави: 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 договорами; об'єкти підвищеної небезпеки (в 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; чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112; аварій-

но-рятувальні служби; Національна система конфіденційного зв'зку; платіжні системи; нерухомі об'єкти культурної спадщини.

Аналіз критеріїв за якими можливо виділити чи ідентифікувати об'єкти КІІ був проведений у [4]. Встановлено, що одні з перших критеріїв ідентифікації КІ були вказані в Директиві ЄС [5]. Відповідно до якої, кожна держава повинна ідентифікувати потенційні КІ, які відповідають вимогам двох основних груп критеріїв – міжгалузевих і галузевих. Міжгалузеві критерії повинні включати в себе: 1) критерії втрати (оцінюються з точки зору потенційного числа загиблих або травмованих); 2) критерії економічних наслідків (оцінюються з точки зору значущості економічних втрат та / або деградації продуктів і послуг, включаючи потенційні екологічні наслідки); 3) критерії впливу на громадськість (оцінюються з точки зору впливу на суспільну довіру, фізичні страждання і порушення повсякденного життя, включаючи втрату важливих послуг). Галузеві критерії повинні враховувати характеристики окремих секторів КІ. Вони визначають характерні риси або функції об'єктів, включених до об'єктів КІ.

У США, згідно [6], прийнято поділяти КІ на ті, що пов'язані з міжнародними організаціями (об'єкти енергетики, транспорт, банківсько-фінансова система, телекомунікації) і ті, які з ними не пов'язані (наприклад, водопостачання, служби порятунку, державне управління). Відповідно до [4], об'єкти КІ поділяються за категоріями наслідків на різні напрями та сектори: економіка, фінанси, навколишнє середовище, здоров'я і безпека, технологічне середовище, тривалість впливу. Також критичність може бути описана трьома загальними характеристиками [7]: критична частка, критичний час та критична якість.

В Україні єдиним переліком критеріїв, які можуть бути використані для ідентифікації об'єктів КІІ є затверджений у [8] перелік негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему (ІТС), до яких належить: 1) виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону); 2) негативний вплив на стан енергетичної безпеки держави; 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; 10) порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави, в тому числі її взаємодії з відповідними інфраструктурами інших держав.

Питаннями захисту КІІ держави займаються такі вітчизняні та закордонні вчені: Х. Алькарас, Д. Бірюков, Д. Бобро, Д. Грітсаліс, О. Довгань, Є. Єлісєєва, А. Кондратьєв, М. Мерабті, Л. Романо, Х. Сятерліс, І. Фовіно, В. Харченко та ін. Проте переважна більшість досліджень не є системними: здебільшого вони орієнтовані на розробку й застосування превентивних та контрзаходів для захисту окремих об'єктів КІ чи КІІ; мало уваги приділяється механізмам формування переліку КІІ держави, а відомі методи й методики (згідно міжнародних стандартів та рекомендованих практик), які не є формалізованими, що ускладнює їх застосування на загальнодержавному рівні, зокрема в авіаційній галузі. З огляду на це мета роботи – на основі розробленої уніфікованої моделі даних сформувати перелік критичних авіаційних інформаційних систем (КАІС) та визначити їх метрики зв'язності та складності.

2. Основна частина дослідження

Серед галузей КІ особливого захисту потребує авіаційна галузь держави, де відповідно до керівних документів (зокрема [9, 10]), необхідно ідентифікувати і захищати КАІС. Адже очевидно, що несанкціоноване втручання у роботу КАІС може призвести до значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури. Проте, жоден із керівних документів ІСАО чи ЕСАС щодо забезпечення захисту міжнародної цивільної авіації не містить повний перелік КАІС, що ускладнює розробку ефективних методів захисту КАІС від різного роду кіберзагроз. Зважаючи на це, була розроблена уніфікована модель даних для формування переліку об'єктів КІІ держави [11–16]. Відповідно до якої, повна множина категорій систем КІІ у певній галузі $\mathbf{S}$ може бути представлена як:

$$\mathbf{S} = \left\{ \bigcup_{i=1}^{n} \mathbf{S}_i \right\} = \{ \mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_n \}, \qquad (1)$$

де $\mathbf{S}_i \subseteq \mathbf{S}$ $(i = \overline{1,n})$ – категорії систем в певній галузі КІ, n – загальна кількість категорій систем.

Множина категорій $\mathbf{S}_i$ може бути представлена у вигляді множини систем:

$$\mathbf{S}_i = \left\{ \bigcup_{j=1}^{m} \mathbf{S}_{ij} \right\} = \{ \mathbf{S}_{i1}, \mathbf{S}_{i2}, \ldots, \mathbf{S}_{im_i} \}, \qquad (2)$$

де $\mathbf{S}_{ij} \subseteq \mathbf{S}_i$ $(i = \overline{1,n},\ j = \overline{1,m_i})$ – системи i-ої категорії, m_i – кількість систем i-х категорій.

Множина систем $\mathbf{S}_{ij}$ може бути представлена у вигляді множини підсистем:

$$\mathbf{S}_{ij} = \left\{ \bigcup_{k=1}^{r_{ij}} \mathbf{S}_{ijk} \right\} = \{ S_{ij1}, S_{ij2}, \ldots, S_{ijr_{ij}} \}, \qquad (3)$$

де $S_{ijk} \subseteq \mathbf{S}_{ij}$ $(i = \overline{1,n},\ j = \overline{1,m_i},\ k = \overline{1,r_{ij}})$ – множина підсистем системи $\mathbf{S}_{ij}$, r_{ij} – кількість підсистем ij-ї системи.

Множина підсистем системи S_{ijk} може бути представлена у вигляді підмножини підсистем:

$$\mathbf{S}_{ijk} = \left\{ \bigcup_{p=1}^{v_{ijk}} \mathbf{S}_{ijkp} \right\} = \{ S_{ijk1}, S_{ijk2}, \ldots, S_{ijkv_{ijk}} \}, \qquad (4)$$

де $S_{ijkp} \subseteq \mathbf{S}_{ijk}$ $(i = \overline{1,n},\ j = \overline{1,m_i},\ k = \overline{1,r_{ij}},\ p = \overline{1,v_{ijk}})$ – підмножина підсистем $\mathbf{S}_{ijk}$, v_{ijk} – кількість підмножин ijk-ої підсистеми.

У залежності від можливостей деталізації категорій галузі КІІ підмножина підсистем S_{ijkp} може бути також представлена у вигляді підмножин з поглибленим рівнем деталізації. Тому існує необхідність представлення повної множини категорій систем у галузі КІІ **S** у загальному вигляді таким чином:

$$\mathbf{S}=\left\{\bigcup_{i_1=1}^{n_0}\left\{\bigcup_{i_2=1}^{n_{i_1}}\left\{\dots\left\{\bigcup_{i_l=1}^{n_{i_1,i_2,\dots,i_{l-1}}}\mathbf{S}_{i_1,i_2,\dots,i_l}\right\}\right\}\right\}\right\}, \quad (5)$$

де $\mathbf{S}_{i_1,i_2,\dots,i_l}\subseteq\mathbf{S}$ $(i_1=\overline{1,n_0}$, $i_2=\overline{1,n_{i_1}}$, $i_l=\overline{1,n_{i_1,i_2,\dots,i_{l-1}}})$ – рівні деталізації категорій систем **S**, l – кількість рівнів деталізації категорій систем.

Для визначення зв'язності отриманих за допомогою уніфікованої моделі даних сформуємо згідно [17] матрицю інцидентності Δ (6), яка для визначеної множини систем КАІС (обраного рівня деталізації) $\mathbf{Y}=\{\bigcup_{i=1}^{m}Y_i\}=\{Y_1,Y_2,\dots,Y_m\}$, де $Y_i\subseteq\mathbf{Y}$ $(i=\overline{1,m})$, де m – загальна кількість систем, та множини кіберзагроз (КЗ) об'єктам КІ держави

$$\mathbf{X}=\left\{\bigcup_{j=1}^{n}X\right\}=\{X_1,X_2,\dots,X_n\},$$

де $X_i\subseteq\mathbf{X}$ $(j=\overline{1,n})$, де n – загальна кількість КЗ відображає відношення впливу λ. Матриця інцидентності визначає відношення $\Delta=(\lambda_{ij})$, що характеризує можливість певної КЗ X_j вплинути на певну систему КАІС Y_i (де $\lambda_{ij}=1$, якщо $(Y_i,X_j)\in 1$, та $\lambda_{ij}=0$, якщо $(Y_i,X_j)\notin 1$).

$$\Delta=(\lambda_{ij})_{(i=\overline{1,m},\,j=\overline{1,n})}, \quad (6)$$

після чого можливо сформувати множини вершин комплексу, що характеризують перелік можливих КЗ для певної системи $K_Y(X;\lambda)$, та перелік систем, на які може вплинуть певна КЗ $K_X(Y;\lambda^{-1})$. При необхідності розгляду комплекс у цілому, доцільно використати поняття ланцюга зв'язку, який відображає той факт, що два симплекси можуть і не мати спільної грані, але можуть бути зв'язані за допомогою послідовності проміжних симплексів. Симплекційний комплекс – це математичне узагальнення поняття планарного графа, що відображає багатомірну природу бінарного відношення системи. Оскільки симплекційний комплекс є множиною симплексів, з'єднаних між собою за допомогою спільних граней, то за характеристику зв'язку можна брати величину грані, спільної для двох симплексів. Отже, якщо множини **Y** та **X** мають m і n елементів відповідно, то матриця Δ є матрицею розміром $(m\times n)$, яка складається з нулів та одиниць. Добуток $\Delta\Delta^T$ – це число, що стоїть на місці (i,j) та є скалярним добутком рядків i та j матриці Δ. Воно дорівнює числу одиниць, що знаходяться на одних і тих самих місцях у рядках i та j матриці Δ і відповідає значенню $(q+1)$, де q – розмірність спільної гарні симплексів σ_p і σ_r, заданих рядками i та j. Таким чином, для знаходження q - спільних граней усіх пар Y-симплексів у $K_Y(X;\lambda)$ необхідно: скласти матрицю $\Delta\Delta^T$ розміром $(m\times m)$; оцінити $\Delta\Delta^T-\Omega$, де $\Omega=(\omega_{ij})$, а $\omega_{ij}=1$ для $i,j=\overline{1,m}$. Цілі числа на діагоналі матриці є розмірностями симплексів Y, а Q-аналіз здійснюється перевіркою інших комбінацій стовпчиків та рядків. Аналіз для $K_X(Y;\lambda^{-1})$ виконується за допомогою складення матриці $\Delta^T\Delta-\Omega'$, де Ω' – матриця розміром $(n\times n)$, що складається з одиниць. Цілі числа на діагоналі матриці також є розмірностями симплексів X, а Q - аналіз здійснюється перевіркою інших комбінацій стовпчиків та рядків. Кількість різних q - зв'язних комбінацій комплексу K позначається через число Q_q, а їх упорядковані в порядку спадання значення є першим структурним вектором комплексу. За допомогою структурного вектору згідно [17] та виразу

$$\varphi(\mathrm{K})=2\left[\sum_{i=0}^{N}(i+1)Q_i\right]\Big/\big((N+1)(N+2)\big),$$

можна отримати і порівняти міру складності комплексів.

На основі запропонованої уніфікованої моделі даних та згідно [18] створено методику (рис. 1), яка дозволяє формувати перелік об'єктів КІІ певної галузі та на загальнодержавному рівні.

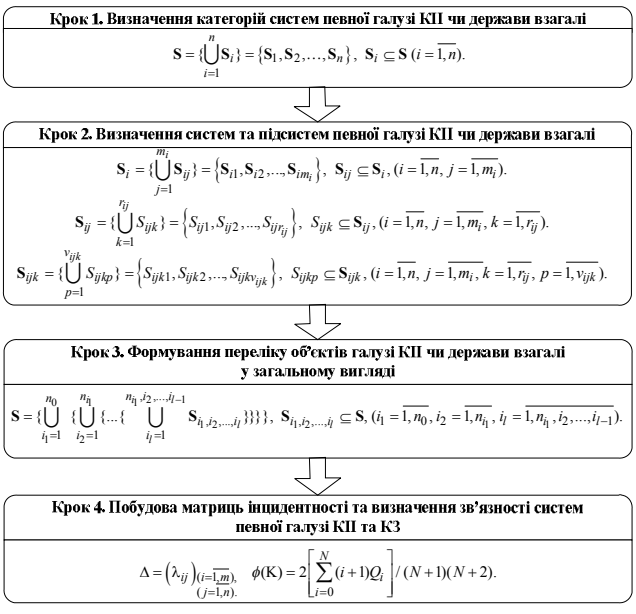

Рис. 1. Методика формування переліку об'єктів галузі КІІ

Методика складається з наступних кроків:

1) Визначення категорій систем певної галузі КІІ чи держави взагалі згідно (1);

2) Визначення систем та підсистем згідно (2)-(4);

3) Формування переліку об'єктів галузі КІІ чи держави взагалі у загальному вигляді на основі (5);

4) Побудова матриць інцидентності та визначення зв'язності систем певної галузі КІІ та КЗ згідно (6).

3. Експериментальне дослідження

Відповідно запропонованої методики, розглянемо приклад формування переліку об'єктів КІІ для авіаційної галузі (на основі системи КАІС) згідно [19], при $n=3$ з урахуванням (1), визначимо множину категорій систем таким чином:

$$\mathbf{S}_{KAIS}=\left\{\bigcup_{i=1}^{3}\mathbf{S}_i\right\}=\{\mathbf{S}_1,\mathbf{S}_2,\mathbf{S}_3\}=\{\mathbf{S}_{ISAO},\mathbf{S}_{BSPS},\mathbf{S}_{ISAA}\},$$

де $\mathbf{S}_1=\mathbf{S}_{ISAO}$ – множина інформаційних систем аеронавігаційного обслуговування; $\mathbf{S}_2=\mathbf{S}_{BSPS}$ – множина бортових інформаційних систем повітряних суден; $\mathbf{S}_3=\mathbf{S}_{ISAA}$ – множина інформаційних систем авіакомпаній та аеропортів згідно [19].

Для множини категорій $\mathbf{S}_1$, при $n=1,\ m_1=5$ з використанням (2), представимо множину систем таким чином:

$$\mathbf{S}_1=\mathbf{S}_{ISAO}=\left\{\bigcup_{j=1}^{5}\mathbf{S}_{1j}\right\}=\{\mathbf{S}_{1.1},\mathbf{S}_{1.2},\mathbf{S}_{1.3},\mathbf{S}_{1.4},\mathbf{S}_{1.5}\}=$$
$$=\{\mathbf{S}_{SAE},\mathbf{S}_{RZZP},\mathbf{S}_{SSP},\mathbf{S}_{SOD},\mathbf{S}_{SMZ}\},$$

де $\mathbf{S}_{1.1}=\mathbf{S}_{SAE}$ – системи авіаційного електрозв'язку; $\mathbf{S}_{1.2}=\mathbf{S}_{RZZP}$ – радіонавігаційні засоби забезпечення польотів; $\mathbf{S}_{1.3}=\mathbf{S}_{SSP}$ – системи спостереження; $\mathbf{S}_{1.4}=\mathbf{S}_{SOD}$ – системи обробки даних; $\mathbf{S}_{1.5}=\mathbf{S}_{SMZ}$ – системи метеорологічного забезпечення [19].

Аналогічно, для множини категорій $\mathbf{S}_2$, при $n=2,\ m_2=7$ з використанням (2), представимо множину систем таким чином:

$$\mathbf{S}_2=\mathbf{S}_{BSPS}=\left\{\bigcup_{j=1}^{7}\mathbf{S}_{1j}\right\}=$$
$$=\{\mathbf{S}_{2.1},\mathbf{S}_{2.2},\mathbf{S}_{2.3},\mathbf{S}_{2.4},\mathbf{S}_{2.5},\mathbf{S}_{2.6},\mathbf{S}_{2.7}\}=$$
$$=\{\mathbf{S}_{SPS},\mathbf{S}_{SZV},\mathbf{S}_{NAVS},\mathbf{S}_{SSPZ},\mathbf{S}_{OSL},\mathbf{S}_{SVI},\mathbf{S}_{ABSK}\},$$

де $\mathbf{S}_{2.1}=\mathbf{S}_{\mathrm{SPS}}$ – система повітряних сигналів; $\mathbf{S}_{2.2}=\mathbf{S}_{\mathrm{SZV}}$ – системи зв'язку; $\mathbf{S}_{2.3}=\mathbf{S}_{\mathrm{NAVS}}$ – навігаційні системи; $\mathbf{S}_{2.4}=\mathbf{S}_{\mathrm{SSPZ}}$ – системи спостереження та попередження зіткнень; $\mathbf{S}_{2.5}=\mathbf{S}_{\mathrm{OSL}}$ – обчислювальні системи літаководіння; $\mathbf{S}_{2.6}=\mathbf{S}_{\mathrm{SVI}}$ – системи відображення інформації; $\mathbf{S}_{2.7}=\mathbf{S}_{\mathrm{ABSK}}$ – автоматичні бортові системи керування [19].

Аналогічно, для множини категорій $\mathbf{S}_3$, при $n=3,\ m_3=5$ з використанням (2), представимо множину систем таким чином:

$$\mathbf{S}_3=\mathbf{S}_{ISAA}=\left\{\bigcup_{j=1}^{5}\mathbf{S}_{1j}\right\}=\{\mathbf{S}_{3.1},\mathbf{S}_{3.2},\mathbf{S}_{3.3},\mathbf{S}_{3.4},\mathbf{S}_{3.5}\}=$$
$$=\{\mathbf{S}_{CRS},\mathbf{S}_{GDS},\mathbf{S}_{IDS},\mathbf{S}_{BSP},\mathbf{S}_{DCS}\},$$

де $\mathbf{S}_{3.1}=\mathbf{S}_{\mathrm{CRS}}$ – система комп'ютерного бронювання; $\mathbf{S}_{3.2}=\mathbf{S}_{\mathrm{GDS}}$ – глобальна система резервування (бронювання); $\mathbf{S}_{3.3}=\mathbf{S}_{IDS}$ – Інтернет системи бронювання (IDS) або альтернативні системи бронювання (ADS); $\mathbf{S}_{3.4}=\mathbf{S}_{BSP}$ – система взаєморозрахунків; $\mathbf{S}_{3.5}=\mathbf{S}_{DCS}$ – системи управління відправками згідно [19].

За допомогою уніфікованої моделі даних було сформовано перелік об'єктів КІІ авіаційної галузі, у результаті чого (при рівні деталізації $l=4$) виділено 3 множини категорій, 17 множин систем, 97 множин підсистем, 125 підсистем КАІС.

Сформований перелік ідентифікованих критичних об'єктів будь-якого рівня деталізації може бути використаний для аналізу впливу можливих КЗ (для прикладу було обрано множини систем $\mathbf{S}_{ij}$ при $l=2$). Побудована, на основі (6), матриця інцидентності відношення $\Delta_{KAIS\_THREATS}$ (рис. 2) при $i=\overline{1,17},\ j=\overline{1,19}$, характеризує можливість певної КЗ X_j вплинути на певну КАІС Y_i. Де Y_i – це визначені за (2) множини систем $\mathbf{S}_{ij}$, а саме: Y_1 – системи авіаційного електрозв'язку; Y_2 – радіонавігаційні засоби забезпечення польотів; Y_3 – системи спостереження; Y_4 – системи обробки даних; Y_5 – системи метеорологічного забезпечення; Y_6 – система повітряних сигналів; Y_7 – системи зв'язку; Y_8 – навігаційні системи; Y_9 – системи спостереження та попередження зіткнень; Y_{10} – обчислювальні системи літаководіння; Y_{11} – системи відображення інформації; Y_{12} – автоматичні бортові системи керування; Y_{13} – система комп'ютерного бронювання; Y_{14} – глобальна система резервування (бронювання); Y_{15} – Інтернет системи бронювання (Internet Distribution Systems, IDS); Y_{16} – система взаєморозрахунків; Y_{17} – системи управління відправками, а відповідно до [2]: X_1 – авіаційні катастрофи; X_2 – ядерні аварії; X_3 – аварії у системах енергозабезпечення; X_4 – викиди небезпечних речовин; X_5 – відмови систем; X_6 – аварії та надзвичайні події обумовлені недбалістю, організаційними помилками; X_7 – аварії на об'єктах підвищенної небезпеки; X_8 – метеорологічні або надзвичайні погодні умови; X_9 – гідрологічні загрози; X_{10} – сейсмічні загрози; X_{11} – геологічні загрози; X_{12} – геліофізичні загрози; X_{13} – пожежі (лісові,степові, торфяні); X_{14} – епідемії та пандемії, епізоотії, епіфітотії; X_{15} – дії терористів; X_{16} – дії злочинців та диверсантів; X_{17} – військові дії в умовах війни; X_{18} – кібератаки на ІТС; X_{19} – загрози функціонування державних органів влади, збройних сил, правоохоронних органів та спецслужб.

	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}
Y_1	1	1	1	0	1	1	0	1	1	1	0	1	0	0	1	1	1	1	0
Y_2	1	0	1	0	1	1	0	1	1	1	0	0	0	0	1	1	1	1	0
Y_3	1	0	0	0	1	1	0	1	1	1	1	1	1	0	1	1	0	1	0
Y_4	1	0	0	0	1	1	0	1	1	1	1	1	0	0	1	1	0	1	0
Y_5	1	1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	0	0	0
Y_6	1	0	1	0	1	0	0	1	1	1	1	1	1	0	1	1	0	0	0
Y_7	1	0	1	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1	1
Y_8	1	0	1	0	1	1	0	1	1	1	1	1	0	0	1	1	1	1	0
Y_9	1	0	1	0	1	1	1	1	1	1	0	1	1	0	1	1	1	1	0
Y_{10}	1	0	0	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0
Y_{11}	1	1	1	0	1	1	0	1	1	1	0	0	0	0	1	0	1	1	0
Y_{12}	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0
Y_{13}	1	0	1	0	1	1	0	1	0	0	0	1	0	1	1	1	1	1	1
Y_{14}	1	0	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	1	1
Y_{15}	1	0	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	1	0
Y_{16}	1	0	1	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0
Y_{17}	1	1	1	1	1	1	0	1	1	0	0	1	1	1	1	1	1	1	1

Рис. 2. Матриця інцидентності $\Delta_{KAIS\_THREATS}$

Згідно матриці інцидентності (рис. 2) сформуємо множину вершин комплексів $K_Y(X;\lambda)$, що характеризують перелік КЗ, які можуть вплинути на певну систему КАІС:

$(Y_1) < X_1, X_2, X_3, X_5, X_6, X_8, X_9, X_{10}, X_{12}, X_{15}, X_{16}, X_{17}, X_{18} > \sigma_{12}$;

$(Y_2) < X_1, X_3, X_5, X_6, X_8, X_9, X_{10}, X_{15}, X_{16}, X_{17}, X_{18} > \sigma_{10}$;

$(Y_3) < X_1, X_5, X_6, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{13}, X_{15}, X_{16}, X_{18} > \sigma_{11}$;

$(Y_4) < X_1, X_5, X_6, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{15}, X_{16}, X_{18} > \sigma_{10}$;

$(Y_5) < X_1, X_2, X_4, X_5, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{13}, X_{16} > \sigma_{10}$;

$(Y_6) < X_1, X_3, X_5, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{13}, X_{15}, X_{16} > \sigma_{10}$;

$(Y_7) < X_1, X_3, X_4, X_5, X_6, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{15}, X_{16}, X_{17}, X_{18}, X_{19} > \sigma_{14}$;

$(Y_8) < X_1, X_3, X_5, X_6, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{15}, X_{16}, X_{17}, X_{18} > \sigma_{12}$;

$(Y_9) < X_1, X_3, X_5, X_6, X_7, X_8, X_9, X_{10}, X_{12}, X_{13}, X_{15}, X_{16}, X_{17}, X_{18} > \sigma_{13}$;

$(Y_{10}) < X_1, X_5, X_6, X_8, X_{10}, X_{16} > \sigma_5$;

$(Y_{11}) < X_1, X_3, X_4, X_5, X_6, X_8, X_9, X_{10}, X_{15}, X_{17}, X_{18} > \sigma_{10}$;

$(Y_{12}) < X_1, X_2, X_3, X_5, X_7, X_8, X_9 > \sigma_6$;

$(Y_{13}) < X_1, X_3, X_5, X_6, X_8, X_{12}, X_{14}, X_{15}, X_{16}, X_{17}, X_{18}, X_{19} > \sigma_{11}$;

$(Y_{14}) < X_1, X_3, X_5, X_6, X_8, X_{14}, X_{15}, X_{16}, X_{18}, X_{19} > \sigma_9$;

$(Y_{15}) < X_1, X_3, X_5, X_6, X_8, X_{14}, X_{15}, X_{16}, X_{18} > \sigma_8$;

$(Y_{16}) < X_1, X_3, X_5, X_6, X_{14}, X_{15}, X_{16}, X_{18} > \sigma_7$;

$(Y_{17}) < X_1, X_2, X_3, X_4, X_5, X_6, X_8, X_9, X_{12}, X_{13}, X_{14}, X_{15}, X_{16}, X_{17}, X_{18}, X_{19} > \sigma_{15}$.

Згідно матриці інцидентності (рис. 2) сформуємо множину вершин комплексів $K_X(Y;\lambda^{-1})$, що характеризують перелік системи, на які може вплинути певна КЗ:

$(X_1) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{16}$;

$(X_2) < y_1, y_5, y_{11}, y_{12}, y_{17} > \sigma_4$;

$(X_3) < y_1, y_2, y_6, y_7, y_8, y_9, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{12}$;

$(X_4) < y_5, y_7, y_{17} > \sigma_2$;

$(X_5) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{16}$;

$(X_6) < y_1, y_2, y_3, y_4, y_7, y_8, y_9, y_{10}, y_{11}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{13}$;

$(X_7) < y_9, y_{12} > \sigma_1$;

$(X_8) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{17} > \sigma_{15}$;

$(X_9) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{11}, y_{12}, y_{17} > \sigma_{11}$;

$(X_{10}) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11} > \sigma_{10}$;

$(X_{11}) < y_3, y_4, y_5, y_6, y_7, y_8 > \sigma_5$;

$(X_{12}) < y_1, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{13}, y_{17} > \sigma_9$;

$(X_{13}) < Y_3, y_5, y_6, y_9, y_{17} > \sigma_4$;

$(X_{14}) < y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_4$;

$(X_{15}) < y_1, y_2, y_3, y_4, y_6, y_7, y_8, y_9, y_{11}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{13}$;

$(X_{16}) < y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{14}$;

$(X_{17}) < y_1, y_2, y_7, y_8, y_9, y_{11}, y_{13}, y_{17} > \sigma_7$;

$(X_{18}) < y_1, y_2, y_3, y_4, y_7, y_8, y_9, y_{11}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17} > \sigma_{12}$;

$(X_{19}) < y_7, y_{13}, y_{14}, y_{17} > \sigma_3$.

Для знаходження q - спільних граней усіх пар Y - симплексів у $K_Y(X;\lambda)$ сформуємо матрицю $\Delta\Delta^T$ розміром $(m \times m)$ (рис. 3).

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	
12	10	9	9	7	8	11	11	11	5	10	5	9	7	7	6	11	Y_1
	10	8	8	5	7	10	10	10	5	9	4	8	7	7	6	9	Y_2
		11	10	8	9	10	10	10	5	7	3	7	6	6	5	9	Y_3
			10	7	8	10	10	9	5	7	3	7	6	6	5	8	Y_4
				10	8	8	7	7	4	5	4	4	3	3	2	8	Y_5
					10	9	9	9	4	6	4	6	5	5	4	8	Y_6
						14	12	11	5	9	4	10	8	7	6	12	Y_7
							12	11	5	9	4	9	7	7	6	10	Y_8
								13	5	9	5	9	7	7	6	11	Y_9
									5	4	2	4	4	4	3	4	Y_{10}
										10	5	7	6	6	5	9	Y_{11}
											6	3	3	3	2	5	Y_{12}
												11	9	8	7	11	Y_{13}
													9	8	7	9	Y_{14}
														8	7	8	Y_{15}
															7	7	Y_{16}
																15	Y_{17}

Рис. 3. Матриця інцидентності системи КАІС

Враховуючи, що розмірність є величиною грані симплексу, отримані значення розмірностей симплексу q (цілі числа на діагоналі) зазначаємо у порядку спадання та визначаємо їх зв'язність та приналежність до систем. Якщо Q – значення симплексів комплексу $K_Y(X;\lambda)$ – системи КАІС, то:

при $q=15, \{Y_{17}\}$, $Q_{15}=1$; при $q=14, \{Y_7\}, Q_{14}=1$;

при $q=13$, $\{Y_9\}$, $Q_{13}=1$; при $q=12, \{Y_1\}\{Y_7, Y_8\}$, $Q_{12}=2$; при $q=11$, $\{Y_3\}\{Y_{13}, Y_{17}\}, Q_{11}=2$;

при $q=10$, $\{Y_1, Y_2, Y_7, Y_8, Y_9\}$ $\{Y_3, Y_4\}\{Y_5\}\{Y_6\}\{Y_{11}\}, Q_{10}=5$;

при $q=9$, $\{Y_{13}, Y_{14}, Y_{17}\}$, $Q_9=1$;

при $q=8$, $\{Y_{13}, Y_{14}, Y_{15}, Y_{17}\}$ $Q_8=1$;

при $q=7, \{Y_{13}, Y_{14}, Y_{15}, Y_{16}, Y_{17}\}, Q_7=1$;

при $q=6, \{Y_{12}\}$, $Q_6=1$;

при $q=5, \{Y_1, Y_2, Y_3, Y_4, Y_7, Y_8, Y_9, Y_{10}\}, Q_5=1$.

Перший структурний вектор комплексу $K_Y(X;\lambda)$ систем КАІС $Q_Y=\{1,1,1,2,2,5,1,1,1,1,1\}$, а міра складності комплексу $\phi_{KAIS}=1,39$. Аналогічно, для знаходження q-спільних граней усіх пар X-симплексів у $K_X\left(Y;\lambda^{-1}\right)$ сформуємо матрицю $\Delta^T\Delta$ розміром $(n\times n)$ (рис. 4).

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	
16	4	12	2	16	13	1	15	11	10	5	9	4	4	13	14	7	12	3	X_1
	4	3	1	4	2	0	4	4	2	0	2	1	0	2	2	2	2	0	X_2
		12	1	12	10	1	11	8	6	2	6	2	4	11	10	7	10	3	X_3
			2	2	1	0	2	2	1	1	2	1	0	1	2	1	1	1	X_4
				16	13	1	15	11	10	5	9	4	4	13	14	7	12	3	X_5
					13	0	12	8	8	3	7	2	4	12	12	7	12	3	X_6
						1	1	1	0	0	0	0	0	0	0	0	0	0	X_7
							15	11	10	5	9	4	3	12	13	7	11	3	X_8
								11	9	5	8	4	0	9	9	6	8	1	X_9
									10	5	7	3	0	8	9	5	7	0	X_{10}
										5	5	2	0	4	5	1	3	0	X_{11}
											9	4	1	8	9	5	7	2	X_{12}
												4	0	3	4	1	2	0	X_{13}
													4	4	4	1	4	2	X_{14}
														13	12	7	12	3	X_{15}
															14	6	11	3	X_{16}
																7	7	2	X_{17}
																	12	3	X_{18}
																		3	X_{19}

Рис. 4. Матриця інцидентності КЗ об'єктам КІ держави

Отримані значення розмірностей симплексу q зазначаємо у порядку спадання та визначаємо їх зв'язність та приналежність до систем.

Якщо Q – значення симплексів комплексу $K_X(Y;\lambda^{-1})$ – кіберзагроз об'єктам критичної інфраструктури держави, то:

при $q=16, \{X_1, X_5\}, Q_{16}=1$;

при $q=15, \{X_1, X_5, X_8\}, Q_{15}=1$;

при $q=14, \{X_1, X_5, X_{16}\}, Q_{14}=1$;

при $q=13, \{X_1, X_5, X_6\}\{X_{15}\}, Q_{13}=2$;

при $q=12, \{X_1, X_3, X_5\}\{X_6, X_{15}, X_{18}\}, Q_{12}=2$;

при $q=11, \{X_1, X_5, X_8, X_9\}, Q_{11}=1$;

при $q=10, \{X_1, X_5, X_8, X_{10}\}, Q_{10}=1$;

при $q=9, \{X_1, X_5, X_8, X_{12}, X_{16}\}, Q_9=1$;

при $q=7, \{X_1, X_3, X_5, X_6, X_8, X_{15}, X_{17}, X_{18}\}, Q_7=1$;

при $q=5, \{X_1, X_5, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{16}\}, Q_5=1$;

при $q=4, \{X_1, X_2, X_5, X_8, X_9\}\{X_{12}, X_{13}, X_{16}\}$

$\{X_3, X_6, X_{14}, X_{15}, X_{18}\}, Q_4=3$.

Перший структурний вектор комплексу $K_X(Y;\lambda^{-1})$ – кіберзагроз об'єктам критичної інфраструктури, буде мати вигляд:

$$Q_X=\{1,1,1,2,2,1,1,1,1,1,3,1,1,1\},$$

а міра складності комплексу $\phi_{THREATS}=1,13$.

Висновки

В роботі на основі раніше розробленої уніфікованої моделі даних було створено методику формування переліку об'єктів КІІ, яка за рахунок мультирівневої деталізації, ієрархічного представлення множин, що характеризують системи та їх компоненти, а також введення матриці інцидентності кібербезпеки КІІ, її симплексних комплексів та Q-аналізу, дозволила сформулювати перелік КАІС та визначити їх зв'язність (співвідношення q-зв'язків множин КЗ та КАІС). Як показало дослідження, відношення q-зв'язків множин КЗ має більш високу зв'язність у порівнянні з аналогічними відношеннями q-зв'язків множин систем КАІС, а це свідчить, що реалізація однієї КЗ може ініціювати каскадний ефект на інші зв'язані загрози та призвести до важких, а іноді і руйнівних наслідків для певної системи КАІС. Крім того, визначені структурні вектори відношення для систем КАІС $Q_Y=\{1,1,1,2,2,5,1,1,1,1,1\}$ та загроз КІ держави $Q_X=\{1,1,1,2,2,1,1,1,1,1,3,1,1,1\}$, за допомогою яких були отримані міри (числові значення) складності комплексів цих відношень. Обчислені міри складності комплексів $\varphi_{KAIS}=1,39$ та $\varphi_{THREATS}=1,13$ свідчать про більшу «складність» систем КАІС. Зауважимо, що таке визначення складності розглядає тільки статистичну складність обраних комплексів. Зазначені результати можуть бути використані відповідними державними органами для формування переліку об'єктів КІІ з метою застосування адекватних методів і засобів захисту.

СПИСОК ЛІТЕРАТУРИ

1. Довгань О. Д. Критична інфраструктура як об'єкт захисту від кібернетичних атак. *Інформаційна безпека: виклики і загрози сучасності* : матеріали наук.-практ. конф. Київ : НА СБ України, 2013. С. 17–20.
2. Зелена книга з питань захисту критичної інфраструктури в України. URL: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf.
3. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.
4. Лядовська В. Методи та критерії ідентифікації об'єктів критичної інфраструктури держави», Мат. VII міжн. НПК «*Інтегровані інтелектуальні робототехнічні комплекси* (ІІРТК-2014)», 19-20 травня 2014 р., Київ, 2014. С. 356–358.
5. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC. URL: http://eur-lex.europa.euLexUriServ/LexUriServ.do?uri=CELEX:32008L0114: EN:HTML:NOT.
6. Цигичко В. Н., Смолян Г. Л., Черешкін Д. С. Забезпечення безпеки критичних інфраструктур в США, т. 27, 2006.
7. Fekete A., Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science.* 2011. Vol. 2, № 1. P.15–24.
8. Постанова Кабінету Міністрів України «Постанова про затвердження порядку формування переліку ІТС об'єктів критичної інфраструктури держави», від 23.08.2016 № 563. URL: http://zak on3.rada.gov.ua/laws/show/563-2016-%D0%BF.
9. Doc 8973 ICAO «Керівництво з авіаційної безпеки» (Restricted), вид. 9, 2014, 818 с.
10. Doc 30 «Політика ECAC у сфері авіаційної безпеки» (Restricted), вид. 13, 2010, 138 с.
11. Гнатюк С., Сидоренко В., Сейлова Н., Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави. *Безпека інформації*. 2017. Том 23, № 2. С. 80–91.
12. Sydorenko V., Zhmurko T., Polishchuk Yu., Gnatyuk S. Data model for forming critical infrastructure objects and determining its connectivity. *Inzynier XXI wieku*, Monografia, Bielsko-Biala, Poland : ATH, 2017. P. 329–350.
13. Sydorenko V., Gnatyuk S., Aleksander M. Unified data model for defining state critical information infrastructure in civil aviation. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies* (DESSERT-2018), 24-27 May. Kyiv, 2018. P. 37–42.
14. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.
15. Amin Salih M., Yuvaraj D., Sivaram M., Porkodi V. Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol. *International Journal of Advanced Research in Computer Science*. Vol. 9, No 6. P. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
16. Gnatyuk S., Zh. Hu, Sydorenko V., Aleksander M., Polishchuk Yu., Yubuzova Kh. Critical Aviation Information Systems: Identification and Protection. *Cases on Modern Computer Systems in Aviation*. USA: IGI Global, 2019. P. 423–448.
17. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Інститут проблем національної безпеки, 2003. 472 с.
18. Сидоренко В. М. Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі. URL: http://er.nau.edu.ua:8080/handle/NAU/33987.
19. Гнатюк С., Васильєв Д. Сучасні критичні авіаційні інформаційні системи. *Безпека інформації*. 2016. Т. 2, № 1. С. 51–57.

REFERENCES

1. Dovgan, O. (2013), "Critical infrastructure as an object of protection against cyber attacks", *Information security: the challenges and threats of our time*, NA SBU, Kyiv, pp. 17–20.
2. *Greeen paper on Critical Infrastructure Protection in Ukraine*, available at: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf.
3. Biryukov, D. and Kondratov, S. (2012), *Protection of critical infrastructure: problems and prospects of implementation in Ukraine: analytical report*, NISS, Kyiv, 96 p.
4. Lyadovska, V. (2014), "Methods and criteria for the identification of objects of the state's critical infrastructure", *Integrated intelligent robotic complexes,* 19-20 May 2014, pp. 356–358.
5. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC, available at: http://eur-lex.europa.euLexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:HTML:NOT.
6. Tsigichko, V., Smolyan, G. and Chereshkin, D. (2006), "Ensuring the safety of critical infrastructures in the USA", T.27.
7. Fekete, A. (2011), "Common criteria for the assessment of critical infrastructures", *International Journal of Disaster Risk Science,* Vol. 2, № 1. pp. 15–24.
8. Resolution on approval of the procedure for the formation of the list of information and telecommunication systems of critical infrastructure objects of the state (2016), available at: http://zakon0.rada.gov.ua/laws/show/563-2016-%D0%BF.
9. Doc 8973 ICAO "Aviation Safety Guide" (2014), no 9, 818 p.
10. Doc 30 «ECAC Policy Statement in the Field of Civil Aviation Facilitation» (2010), T. 13, 138 p.
11. Gnatyuk, S., Sydorenko, V. and Seilova, N. (2017), "Universal data model for the formation of the critical information infrastructure of the state objects list", *Ukrainian Scientific Journal of Information Security,* Vol. 23 (2), pp. 80–91.
12. Sydorenko, V., Zhmurko, T., Polishchuk, Yu. and Gnatyuk, S. (2017), "Data model for forming critical infrastructure objects and determining its connectivity", *Inzynier XXI wieku*, Bielsko-Biala, ATH, Poland, pp. 329–350.
13. Sydorenko, V., Gnatyuk, S. and Aleksander, M. (2018), "Unified data model for defining state critical information infrastructure in civil aviation", *The 9th IEEE Int. Conf. on Dependable Systems, Services and Technologies*, Kyiv, pp. 37–42.
14. Kuchuk, G.A., Kovalenko, A.A. and Mozhaev A.A. (2010), "An Approach To Development Of Complex Metric For Multiservice Network Security Assessment", *Statistical Methods Of Signal and Data Processing* (SMSDP – 2010), Proc. Int. Conf., October 13-14, 2010,: IEEE Ukraine section joint SP, NAU, RED, Kyiv, pp. 158–160.

15. Amin Salih, M., Yuvaraj, D., Sivaram, M. and Porkodi, V. (2018), "Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol", *International Journal of Advanced Research in Computer Science*, Vol. 9, No 6, pp. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
16. Gnatyuk, S., Hu, Zh., Sydorenko, V., Aleksander, M., Polishchuk, Yu. and Yubuzova, Kh. (2019), "Critical Aviation Information Systems: Identification and Protection", *Cases on Modern Computer Systems in Aviation*, IGI Global, USA, pp. 423–448.
17. Kachinsky, A. (2003), *Security, threats and risks: scientific concepts and mathematical methods*, Kyiv, 472 p.
18. Sydorenko, V. (2018), *Methods for critical information infrastructure objects identification and cybersecurity assessment in aviation*, available at: http://er.nau.edu.ua:8080/handle/NAU/33987.
19. Gnatyuk, S. and Vasyliev, D. (2016), "Modern critical aviation information systems", *Information Security*, Vol. 22, Issue 1, pp. 51–57.

Received (Надійшла) 11.04.2019
Accepted for publication (Прийнята до друку) 05.06.2019

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Сидоренко Вікторія Миколаївна – кандидат технічних наук, старший викладач кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна;
Viktoriia Sydorenko – PhD, Senior lecturer of IT-Security Academic Department, National Aviation University, Kyiv, Ukraine;
e-mail: v.sydorenko@ukr.net; ORCID ID: http://orcid.org/0000-0002-5910-0837

Поліщук Юлія Ярославівна – аспірант кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна;
Yuliia Polishchuk – PhD student of IT-Security Academic Department, National Aviation University, Kyiv, Ukraine;
e-mail: polishchuk.yu.ya@gmail.com; ORCID ID: http://orcid.org/0000-0002-0686-2328

Гнатюк Сергій Олександрович – доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна;
Sergiy Gnatyuk – D.Sc., Associate Professor, Professor of IT-Security Academic Department, National Aviation University, Kyiv, Ukraine;
e-mail: s.gnatyuk@nau.edu.ua; ORCID ID: http://orcid.org/0000-0003-4992-0564

Формирование перечня критических авиационных информационных систем в условиях реализации киберугроз

В. Н. Сидоренко, Ю. Я. Полищук, С. А. Гнатюк

Аннотация. Предмет статьи – методы, модели и методики формирования перечня объектов критической информационной инфраструктуры (КИИ). **Цель данной статьи –** на основе разработанной унифицированной модели данных сформировать перечень критических авиационных информационных систем (КАИС) и определить их метрики связности и сложности. **Результаты.** На основе ранее разработанной авторами унифицированной модели данных была создана методика формирования перечня объектов КИИ, которая за счет мультиуровневой детализации, иерархичного представления множеств, характеризующих системы и их компоненты, а также введение матрицы инцидентности кибербезопасности КИИ, ее симплексных комплексов и Q-анализа, позволила сформулировать перечень КАИС и определить их связность (соотношение q-связей множеств киберугроз (КУ) и КАИС). **Выводы.** Проведенное исследование показало, что отношение *q*-связей множества КУ имеет более высокую связность по сравнению с аналогичным отношениям *q*-связей множества систем КАИС, а это свидетельствует, что реализации одной КУ может инициировать каскадный эффект на другие связанные угрозы и привести к тяжелым, а иногда и разрушительным последствиям для определенной системы КАИС. Кроме того, вычисленные степени сложности комплексов $\varphi_{KAIS} = 1{,}39$ и $\varphi_{THREATS} = 1{,}13$ свидетельствуют о большей «сложности» систем КАИС. Указанные результаты могут быть использованы соответствующими государственными органами для формирования перечня объектов КИИ с целью применения адекватных методов и средств защиты.

Ключевые слова: критическая инфраструктура; критическая информационная инфраструктура; критические авиационные информационные системы; киберугрозы; симплексы; матрица инцидентности.

Formation of the list of critical aviation information systems in the context of the cyber threats activities

V. Sydorenko, Yu. Polishchuk, S. Gnatyuk

Abstract. The subject of the paper is the methods and models of forming the list of objects of critical information infrastructure (CII). **The purpose** of this paper is to form a list of critical aviation information systems (CAIS) on the basis of the developed unified data model and determine their metrics of connectivity and complexity. **Results.** Based on the author's previously developed unified data model, a methodology was developed for creating a list of CII objects. It due to multi-level detail, hierarchical representation of sets characterizing systems and their components, as well as the introduction of the incidence matrix of CII cybersecurity, its simplex complexes and Q-analysis, allowed to formulate the list of CAIS and to determine their connectivity (the ratio of *q*-bonds between sets cyber threats (CT) and CAIS). **Conclusions.** This research study has shown that the relations *q*-connections of sets of CT have a higher connectivity in comparison with similar relations *q*-connections of sets of systems of CAIS, which indicates that the implementation of one CT can initiate a cascade effect on other related threats and lead to damage, and sometimes devastating consequences for a certain system of CAIS. In addition, the complexity measurements of complexes $\varphi_{KAIS} = 1{,}39$ and $\varphi_{THREATS} = 1{,}13$ are calculated and indicate a greater «complexity» of CAIS systems. Given results can be used by the relevant state authorities to build a list of CII objects in order to apply adequate security methods and means.

Keywords: critical infrastructure; critical information infrastructure; critical aviation information systems; cyber threats; simplexes; incidence matrix.