УДК 004.056

ФОРМУВАННЯ МНОЖИНИ ІДЕНТИФІКАТОРІВ ДЛЯ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Корченко О.Г. д.т.н., професор,
зав. каф. безпеки інформаційних технологій
Національного авіаційного університету

Дрейс Ю.О. к.т.н., доцент,
зав. каф. інноваційних технологій професійної освіти
Національного авіаційного університету
dreisyuri@gmail.com

Романенко О.О. магістрант,
каф. комп'ютеризованих систем захисту інформації
Національного авіаційного університету
olya_olek@ukr.net

Анотація. *Автоматизація процесів надання послуг у всіх сферах забезпечення життєдіяльності людини, суспільства і держави призвела до посилення вимог щодо захисту інформаційно-телекомунікаційних систем (ІТС) у функціонуванні будь-якої організації, як об'єкта критичної інфраструктури (ОКІ). Для існуючого нормативно-правового забезпечення, пов'язаного з ОКІ, характерна неповнота щодо їх класифікації, не сформований перелік ІТС таких об'єктів, відсутні критерії щодо визначення оцінки негативних наслідків, яка б дозволила сформувати класифікатор об'єктів критичної інформаційної інфраструктури (ОКІІ), що дасть можливість створити умови щодо підвищення стійкості до кібератак. Тому для вирішенням зазначених питань пропонується засіб класифікації ОКІ. В основу його побудови закладена кортежна модель, складовими якої є низка упорядкованих ідентифікаторів, що відображають: сектори критичної інформаційної інфраструктури, форму власності ОКІІ, види інформації, негативні наслідки кібератак на ІТС, тощо. Дана модель надасть можливість провести класифікацію ОКІІ держави та сформувати перелік їх ІТС для забезпечення першочергового захисту від кібератак.*

Ключові слава: *інформаційно-телекомунікаційна система, кібератака, об'єкти критичної інформаційної інфраструктури, класифікатор, кортежна модель.*

Основними нормативно-правовими документами, що регулюють сферу захисту критичну інформаційну інфраструктуру держави (КІІД) є Закон України «Про основи забезпечення кібербезпеки України» [1], Постанова КМУ «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» (далі – Порядок) від 23 серпня 2016 р. №563 [2], а також є й інші документи у сфері забезпечення захисту інформації (ЗІ) та кібербезпеки. Так, у Порядку [2] наголошується на тому, що державні органи, органи центральної виконавчої влади, інші заінтересовані державні органи (далі – заінтересовані органи) повинні сформувати та подати Державній службі спеціального зв'язку та захисту інформації (Держспецзв'язку) пропозиції для формування переліку інформаційно-телекомунікаційних систем (ІТС) об'єктів критичної інфраструктури держави. У відповідності до цих пропозицій заінтересовані органи мають визначити негативні наслідки та вказати їх умовне позначення, до яких може призвести кібератака на ІТС із приведеного у Порядку [2] переліку та зазначити вид інформації, що обробляється в цій системі. Проте, було виявлено неможливість виконання цієї постанови, оскільки у пункті 8 цього Порядку потрібно доповнити перелік критеріїв щодо визначення оцінки негативних наслідків, до яких може призвести кібератака на ІТС об'єкта критичної

інфраструктури, що зазначено у [3-7] і також у листі [8] Інтернет-Асоціації України №32 від 28.02.2017 Президенту України щодо Рішення РНБО від 29.12.2016 «Про загрози кібербезпеці держави та невідкладні заходи їх нейтралізації».

Існуюче нормативно-правове забезпечення захисту об'єктів критичної інфраструктури в інформаційній сфері свідчить про наявність низки проблем [3,4], що мають малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість формування переліку інформаційно-телекомунікаційних систем (ІТС) ОКІ. Крім, того на концептуальному та нормативному рівнях не проведено класифікацію об'єктів критичної інформаційної інфраструктури (ОКІІ), не сформовано переліку ІТС таких об'єктів [5], відсутні критеріїв щодо визначення оцінки негативних наслідків, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури держави тощо [6-8]. Для вирішення цього питання актуальним є розробка необхідного інструментального засобу призначеного для класифікації об'єктів критичної інфраструктури.

Аналіз існуючої моделі даних для формування переліку ОКІІ [9], показав наявне обмеження у її застосуванні,тобто лише до ОКІІ в галузі цивільної авіації (на основі системи критичних авіаційних інформаційних систем), а також не всі враховуються вимоги Порядку [2] до формування переліку ІТС ОКІ, або до переліку критичної інформаційної інфраструктури держави (КІІД). Так, наприклад вимоги до встановлення виду інформації, яка обробляється в ІТС та негативного наслідку до якої може призвести кібератака на ІТС, у моделі [9] невраховані.

Виходячи з вищевикладеного, **метою** роботи є побудова базової кортежної моделі класифікатора ОКІІ, семантика якої використовує умовні позначення ідентифікаторів таких об'єктів за визначеним Порядком [2] їх формування, що дасть можливість провести загальнодержавну класифікацію ОКІІ та сформувати перелік їх ІТС для забезпечення їх захисту від кібератак.

Крім того в [2] КІ включено до переліку ІТС ОКІ, які є складовою КІІД, що у першу чергу (пріоритетно) захищається від кібератак.

На основі проведеного аналізу відповідної нормативно-правової бази та інших праць [1-12] пропонується базова кортежна модель для класифікації ОКІІ держави, яка містить основні ідентифікатори об'єкта:

$$\mathbf{ID} = < \mathbf{ID_1}, \mathbf{ID_2}, ..., \mathbf{ID_i}, ..., \mathbf{ID_n} >, \tag{1}$$

де $\mathbf{ID_i} \subseteq \mathbf{ID}$ $(i = \overline{1,n})$ – компонент кортежу, що відображає *i*-й ідентифікатор об'єкта, а *n* їх кількість.

Наприклад, для формування переліку ІТС ОКІ держави відповідно до [1-3, 10,11], при *n* = 8 кортеж (1) визначимо як:

$$\mathbf{ID} = < \mathbf{ID_1}, \mathbf{ID_2}, \mathbf{ID_3}, \mathbf{ID_4}, \mathbf{ID_5}, \mathbf{ID_6}, \mathbf{ID_7}, \mathbf{ID_8} > = < \mathbf{S}, \mathbf{U}, \mathbf{O}, \mathbf{N}, \mathbf{I}, \mathbf{R}, \mathbf{H}, \mathbf{M} >, \tag{2}$$

Перший компонент кортежу **S** – сектор КІ може бути представлений у вигляді множини секторів:

$$\mathbf{S} = \{\bigcup_{i=1}^{n_1} \mathbf{S_i}\} = \{\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_{n_1}}\}, \tag{3}$$

де $\mathbf{S_i} \subseteq \mathbf{S}$ $(i = \overline{1,n_1})$ – *i*-та підмножина груп ідентифікаторів секторів КІ, а n_1 – загальна кількість груп. Для *i*-ї підмножини $\mathbf{S_i}$ визначимо як:

$$\mathbf{S_i} = \{\bigcup_{j=1}^{n_{1i}} S_{ij}\} = \{S_{i1}, S_{i2}, \ldots, S_{in_{1i}}\}, \tag{4}$$

де $S_{ij} \subseteq \mathbf{S_i}$ $(j = \overline{1,n_{1i}})$ – ідентифікатори секторів *i*-ї групи, а n_{1i} – їх кількість. З урахуванням (4) вираз (3) можна представити у такому вигляді:

$$\mathbf{S} = \{\bigcup_{i=1}^{n_1}\mathbf{S_i}\} = \{\bigcup_{i=1}^{n_1}\{\bigcup_{j=1}^{n_{1i}} S_{ij}\}\} = \{\{S_{11}, S_{12}, \ldots, S_{1n_{11}}\}, \{S_{21}, S_{22}, \ldots, S_{2n_{12}}\}, \ldots, \{S_{n_11}, S_{n_12}, \ldots, S_{n_1n_{1n_1}}\}\}, (i = \overline{1, n_1},\ j = \overline{1, n_{1i}}). \quad (5)$$

Наступний компонент **U** – множина ідентифікаторів адміністративно-територіальних одиниць України, в межах якої знаходиться ОКІ і відображається як:

$$\mathbf{U} = \{\bigcup_{i=1}^{n_2} U_i\} = \{U_1, U_2, ..., U_{n_2}\} = \{"01", "02", "03", ..., "n_2"\}, \quad (6)$$

де $U_i \subseteq \mathbf{U}$ $(i = \overline{1, n_2})$ – ідентифікатор адміністративно-територіальної одиниці, а n_2 – їх загальна кількість.

Відповідно до [12] в Україні наявні 24 області, Автономна Республіка Крим,місто з особливим статусом Севастополь і столиця України – містоКиїв, тому ідентифікатори адміністративно-територіальних одиниць, як і у випадку з **S** можуть бути цифрові або лінгвістичні.

Наприклад, при $n_2 = 27$, $(i = \overline{1, 27})$ з урахуванням [12], формула (6) набере вигляду:

$$\mathbf{U} = \{\bigcup_{i=1}^{27} U_i\} = \{U_1, U_2, U_3, U_4, U_5, U_6, U_7, U_8, U_9, U_{10}, U_{11}, U_{12}, U_{13}, U_{14}, U_{15}, U_{16}, U_{17}, U_{18}, U_{19}, U_{20}, U_{21}, U_{22}, U_{23}, U_{24}, U_{25}, U_{26}, U_{27}\} = \{"01", "02", ..., "26", "27"\} = \quad (7)$$

= {"Автономна Республіка Крим", "Вінницька область",…,"м. Київ", "м. Севастополь"}.

де $U_1 =$ "01"="Автономна Республіка Крим"; $U_2 =$ "02"= "Вінницька область";…; $U_{26} =$ "26"="м. Київ"; $U_{27} =$"27"= "м. Севастополь".

Третій компонент **O** – множина форм власності організації-власника/розпорядника ІТС представляється виразом:

$$\mathbf{O} = \{\bigcup_{i=1}^{n_3} O_i\} = \{O_1, O_2, ..., O_{n_3}\}, \quad (8)$$

де $O_i \subseteq \mathbf{O}$ $(i = \overline{1, n_3})$ – *i*-та форма власності, а n_3 – їх кількість.

Відомо, що за формою власності організації (підприємства, установи) поділяються на державні (Д), колективні (К) та приватні (П).

Наприклад, при $n_3 = 3$, $(i = \overline{1, 3})$ з урахуванням [13],формула (8) матиме вигляд:

$$\mathbf{O} = \{\bigcup_{i=1}^{3} O_i\} = \{O_1, O_2, O_3\} = \{"Д", "К", "П"\}. \quad (9)$$

де, $O_1 =$"*Д*"= "Державні", $O_2 =$"*К*"="Колективні ", а $O_3 =$"*П*"="Приватні".

Черговий компонент **N** – множина назв організацій (підприємств, установ) власників/розпорядників ІТС, як ОКІІ визначається виразом:

$$\mathbf{N} = \{\bigcup_{i=1}^{n_4} N_i\} = \{N_1, N_2, ..., N_{n_4}\}, \quad (10)$$

де $N_i \subseteq \mathbf{N}$ $(i = \overline{1, n_4})$ – *i*-та назва організації (підприємства, установи), а n_4 – їх кількість.

Наприклад, при $n_4 = 5$, $(i = \overline{1, 5})$ формулу (10) можна представити як:

$$\mathbf{N} = \{\bigcup_{i=1}^{5} N_i\} = \{N_1, N_2, N_3, N_4, N_5\} =$$

={"Приват банк", "Ощадбанк", "Укрсоцбанк", "Укргазбанк", "Райффайзен банкаваль"}= (11)
= {"https://privatbank.ua", "https://www.oschadbank.ua", "https:// www.ukrsotsbank.com", "https://www.ukrgasbank.com", "https://aval.ua"}.

Слід зазначити, що назва організації (підприємства, установи) у вигляді лінгвістичного ідентифікатора ″Приват Банк″ може відображатись і гіперпосиланням на офіційний веб-сайт (″https://privatbank.ua″).

П’ятий компонент **R** – множина реєстраційних номерів атестатів відповідності на комплексну систему захисту інформації (КСЗІ) або/та експертних висновків для засобів технічного (криптографічного) ЗІ / організаційно-технічного рішення (ОТР) на КСЗІ, яка відображається виразом:

$$\mathbf{R} = \{\bigcup_{i=1}^{n_5} R_i\} = \{R_1, R_2, ..., R_{n_5}\}, \tag{12}$$

де $R_i \subseteq \mathbf{R}$ $(i = \overline{1, n_5})$ – *i*-й реєстраційний номер атестату відповідності на КСЗІ та/або експертного висновку на ТЗІ/ОТР, а n_5 – їх кількість.

Шостим компонентом кортежу **I** є множина видів інформації, що обробляється в ІТС, яка представляється виразом:

$$\mathbf{I} = \{\bigcup_{i=1}^{n_6} I_i\} = \{I_1, I_2, ..., I_{n_6}\}, \tag{13}$$

де $I_i \subseteq \mathbf{I}$ $(i = \overline{1, n_6})$ – *i*-й ідентифікатор виду інформації, а n_6 – їх кількість. Відповідно до [6, 13] за видом інформація поділяється на: конфіденційну інформацію (КІ), службову інформацію (СІ) та таємну інформацію (ТІ).

Наприклад, при $n_6 = 3$, $(i = \overline{1,3})$ з урахуванням [6, 13],формула (13) матиме вигляд:

$$\mathbf{I} = \{\bigcup_{i=1}^{3} I_i\} = \{I_1, I_2, I_3\} = \{"KI", "CI", "TI"\}, \tag{14}$$

де $I_1 = "KI"$, $I_2 = "CI"$, а $I_3 = "TI"$.

Наступний компонент кортежу **H** – множина ідентифікаторів негативних наслідків кібератак на ІТС, набуває вигляду:

$$\mathbf{H} = \{\bigcup_{i=1}^{n_7} H_i\} = \{H_1, H_2, ..., H_{n_7}\}, \tag{15}$$

де $H_i \subseteq \mathbf{H}$ $(i = \overline{1, n_7})$ – ідентифікатор негативних наслідків, а n_7 – їх кількість.

Наприклад, при $n_7 = 10$, $(i = \overline{1,10})$ з урахуванням [2, 5], формула (15) матиме вигляд:

$$\begin{aligned} \mathbf{H} = \{\bigcup_{\mathbf{i=1}}^{10} H_i\} = \{\mathbf{H_1}, \mathbf{H_2}, \mathbf{H_3}, H_4, H_5, H_6, H_7, H_8, H_9, H_{10}\} = \\ = \{"01", "02", "03", "04", "05", "06", "07", "08", "09", "10"\}, \end{aligned} \tag{16}$$

де $H_1 = "01"$ = ″Виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону)″, $H_2 = "02"$ =″Негативний вплив на стан енергетичної безпеки держави (регіону)″, …, $H_{10} = "10"$ = ″Порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав″. Слід зазначити, що негативні наслідки кібератак на ІТС, як і у випадку з **S**, можуть бути цифрові або лінгвістичні.

Останній компонент **M** – множина ідентифікаторів геолокаційних ресурсів за місцем знаходження організації (підприємства, установи) як ОКІІ:

$$\mathbf{M} = \{\bigcup_{i=1}^{n_8} M_i\} = \{M_1, M_2, ..., M_{n_8}\}, \tag{17}$$

де $M_i \subseteq \mathbf{M}$ $(i = \overline{1, n_8})$ – *i*-й ідентифікатор геолокаційних ресурсів, а n_8 – їх кількість.

Наприклад, при $n_8 = 3$, $(i = \overline{1,3})$ формула (17) набуде вигляду:

$$\mathbf{M} = \{\bigcup_{i=1}^{3} M_i\} = \{M_1, M_2, M_3\} = \{"GM","MM","YM"\}, \quad (18)$$

де $M_1 = "GM"$ = Google Maps, $M_2 = "MM"$ = MAPS.ME , $M_3 = "YM"$ = Yandex Maps.

Висновок.У даному дослідженні запропоновано базову модель класифікатора ОКІІ держави для вирішення наявної проблеми формування переліку ІТС об'єктів критичної інфраструктури, яка за рахунок ідентифікуючих множин параметрів цих об'єктів введених у кортеж дала змогу семантично представити його у вигляді класифікатора, що може бути подальшим практичним механізмом у формуванні переліку ІТС об'єктів критичної інформаційної інфраструктури України.

Література

1."Про основні засади забезпечення кібербезпеки України" Верховна Рада України, Закон України від 05.10.2017р. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.

2."Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави," Кабінет Міністрів України; Постанова, Порядок від 23.08.2016 № 563. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/563-2016-п

3.A. Korchenko, Y. Dreis, O. Romanenko, "Analysis problems in the field of state's critical infrastructure", Projekt interdyscyplinarny projektem XXI wieku: Monografia. Tom 1. – Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2017. – pp.397 - 402.

4.Д. Бірюков, С. Кондратов, О. Суходоля, "Зелена книга з питань захисту критичної інфраструктури в Україні". – К: НІСД, С. 176, 2016. [Електронний ресурс]: Режим доступу: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf

5. Ю. Дрейс "Аналіз базової термінології і негативних наслідків кібератак наінформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", Захист інформації. – 2017. – Т. 19, № 3. – С.214-222.

6.О. Корченко, О. Архипов, Ю. Дрейс, "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія", К.: Наук.-вид. центр НА СБ України, 332 с., 2014, ISBN 978-617-7092-26-0.

7.Ю. Дрейс, О. Романенко "Розширення базової термінології у сфері захисту критичної інформаційної інфраструктури держави", Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті: Матеріали Всеукраїнської науково-практичної інтернет-конференції, 16-17 листопада 2017. – Кропивницький: ЦНТУ, 2017. – 185 с.

8.Лист №32 від 28.02.2017 Президенту України щодо Рішення РНБО від 29.12.2016 "Про загрози кібербезпеці держави та невідкладні заходи їх нейтралізації"від Інтернет-Асоціації України. [Електронний ресурс]. Режим доступу: http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-29122016-pro-zagrozy.

9. С. Гнатюк, В. Сидоренко, Н. Сєйлова, "Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави", Безпека інформації, Том 23, № 2(2017 р). – С. 87 – 91.

10. "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах,"Кабінет Міністрів України, Постанова від 29 березня 2006 р. №373. [Електронний ресурс]. Режим доступу:http://zakon0.rada.gov.ua/laws/show/373-2006-п

11. "Про затвердження Положення про державну експертизу в сфері технічного захисту інформації", Адміністрація Держспецзвязку, Наказ № 93 від 16.03.2007 [Електронний ресурс]. Режим доступу: http://zakon0.rada.gov.ua/laws/show/z0820-07

12. Регіони України: http://static.rada.gov.ua/zakon/new/NEWSAIT/ADM/zmist.html.

13. О. Корченко, Ю. Дрейс "Охорона конфіденційної інформації підприємства": Навчальний посібник. – Житомир: ЖВІ НАУ, 2011. – 172 с.