DOI: 10.18372/2410-7840.20.12448
УДК 004.056

МОДЕЛЬ КЛАСИФІКАТОРА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Олександр Корченко, Юрій Дрейс, Ольга Романенко, Володимир Бичков

Автоматизація процесів надання послуг в усіх сферах забезпечення життєдіяльності людини, суспільства і держави призвела до посилення вимог до захисту інформації в інформаційно-телекомунікаційних системах (ІТС) потенційно небезпечних об'єктів критичної інфраструктури. Відповідно до існуючого нормативно-правового забезпечення, пов'язаного з об'єктами критичної інфраструктури, прослідковується неповнота щодо можливості їх коректної класифікації, також не сформований перелік ІТС таких об'єктів, відсутні критерії щодо оцінювання негативних наслідків від кібератак. Вирішення зазначених питань дозволить сформувати такий класифікатор об'єктів критичної інформаційної інфраструктури, який дасть можливість створити умови для підвищення їх стійкості до кібератак. Відповідно до цього пропонується засіб класифікації об'єктів критичної інформаційної інфраструктури. В основу його побудови закладена кортежна модель, складовими якої є упорядковані ідентифікатори об'єктів критичної інфраструктури, що відображають: сектор критичної інформаційної інфраструктури держави; адміністративно-територіальну одиницю України; назву або ідентифікаційний номер юридичної особи; форму власності організації-власника/розпорядника ІТС; вид інформації, що обробляється в ІТС; реєстраційні номери документів, що засвідчують наявність атестованих/ліцензованих систем чи засобів захисту інформації; негативні наслідки кібератак на ІТС. За допомогою запропонованої моделі представлені приклади класифікації об'єктів критичної інформаційної інфраструктури держави, а в подальшому вона дасть можливість сформувати перелік відповідних ІТС для забезпечення їх першочергового захисту від кібератак.

Ключові слова: *інформаційно-телекомунікаційна система, кібератака, критична інформаційна інфраструктура, класифікатор об'єктів, кортежна модель, негативні наслідки.*

Актуальність. Основними нормативно-правовими документами, що регулюють сферу захисту критичної інформаційної інфраструктури (КІІ) держави є Закон України «Про основи забезпечення кібербезпеки України» [1], а також [2] та інші документи у сфері забезпечення захисту інформації (ЗІ) та кібербезпеки. Так у [2] наголошується на тому, що державні органи, органи центральної виконавчої влади, інші заінтересовані державні органи (далі – заінтересовані органи) повинні сформувати та подати Держспецзв'язку пропозиції для формування переліку ІТС об'єктів критичної інфраструктури (ОКІ) 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 [2] переліку та зазначити вид інформації, що обробляється в цій системі. Проте, було виявлено неможливість виконання цієї постанови, оскільки у пункті 8 [2] потрібно доповнити перелік критеріїв щодо визначення оцінки негативних наслідків, до яких може призвести кібератака на ІТС ОКІ, що зазначається у [3-8].

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

Аналіз існуючої моделі даних 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 враховані всі вимоги [2] до формування переліку ІТС ОКІ, тобто до формування переліку КІІ держави. Так, наприклад, вимоги до встановлення виду інформації, яка обробляється в ІТС та негативних наслідків до яких може призвести кібератака на ІТС, у моделі [9] не враховані.

Виходячи з викладеного **метою роботи** є побудова моделі класифікатора ОКІІ, семантика якої використовує умовні позначення ідентифікаторів таких об'єктів за визначеним у [2] порядком їх формування. Це дасть можливість провести загальнодержавну класифікацію ОКІІ та сформувати перелік відповідних ІТС для забезпечення їх першочергового захисту від кібератак.

Виклад основного матеріалу. У сфері захисту критичної інфраструктури держави в [1-3] введені такі поняття: *ОКІІ* – комунікаційна або технологічна система ОКІ, кібератака на яку безпосередньо вплине на стале функціонування такого ОКІ [1]; 1) *КІІ* – сукупність ОКІІ [3]; 2) включені до переліку ІТС ОКІ, що захищається від кібератак у першу чергу (пріоритетно) [2].

На основі проведеного аналізу відповідної нормативно-правової бази та інших публікацій [1-16] пропонується базова кортежна модель для класифікації ОКІІ держави, яка містить основні ідентифікатори об'єкта:

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

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

Наприклад, для формування переліку ІТС ОКІ держави відповідно до [1-3, 10, 11, 14-16], при $n = 8$ кортеж (1) визначимо як:

$$\begin{gathered}\mathbf{ID} = < \mathbf{ID_1}, \mathbf{ID_2}, \mathbf{ID_3}, \mathbf{ID_4}, \mathbf{ID_5}, \mathbf{ID_6}, \\ \mathbf{ID_7}, \mathbf{ID_8} > = < \mathbf{S}, \mathbf{U}, \mathbf{O}, \mathbf{N}, \mathbf{I}, \mathbf{R}, \mathrm{C}, \mathbf{M} >,\end{gathered} \qquad (2)$$

де $\mathbf{ID_1} = \mathbf{S}$ (множина ідентифікаторів секторів (*Sectors*) КІ); $\mathbf{ID_2} = \mathbf{U}$ (множина ідентифікаторів адміністративно-територіальних одиниць (*Units*) України); $\mathbf{ID_3} = \mathbf{O}$ (множина форм власності (*Ownership*) організації-власників/розпорядників ІТС); $\mathbf{ID_4} = \mathbf{N}$ (множина назв або/та унікальних ідентифікаційних номерів (*Number*) юридичної особи в Єдиному державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників/розпорядників ІТС як ОКІІ); $\mathbf{ID_5} = \mathbf{I}$ (множина видів інформації (*Information*), що обробляється в ІТС); $\mathbf{ID_6} = \mathbf{R}$ (множина реєстраційних номерів (*Registration*) документів, що засвідчують наявність атестованих/ліцензованих систем чи засобів захисту інформації (наприклад, атестатів відповідності на комплексну систему захисту інформації (КСЗІ), комплекс засобів захисту інформації (КЗЗІ), систему управління інформаційної безпеки (СУІБ) або експертних висновків на технічні та програмні засоби, які реалізують функції ТЗІ та/або оцінки стану ЗІ (далі – засоби ТЗІ) чи на організаційно-технічне рішення (ОТР) на розгортання типової складової компоненти КСЗІ в ІТС) та інші; $\mathbf{ID_7} = \mathbf{C}$ (множина ідентифікаторів негативних наслідків (*Consequences*) кібератак на ІТС); $\mathbf{ID_8} = \mathbf{M}$ (множина ідентифікаторів геолокаційних ресурсів (*Maps*) за місцем знаходження ОКІІ).

Перший компонент кортежу $\mathbf{S}$ – сектор КІ може бути представлений у вигляді множини секторів:

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

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:

$$\mathbf{S_i} = \{\bigcup_{j=1}^{n_{1i}} S_{ij}\} = \{S_{i1}, S_{i2}, ..., S_{in_{1i}}\}, \qquad (4)$$

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:

$$\begin{gathered}\mathbf{S} = \{\bigcup_{i=1}^{n_1} \mathbf{S_i}\} = \{\bigcup_{i=1}^{n_1} \{\bigcup_{j=1}^{n_{1i}} S_{ij}\}\} = \\ \{\{S_{11}, S_{12}, ..., S_{1n_{11}}\}, \{S_{21}, S_{22}, ..., S_{2n_{12}}\}, ..., \\ \{S_{n_1 1}, S_{n_1 2}, ..., S_{n_1 n_{1n_1}}\}\}, (i = \overline{1, n_1},\ j = \overline{1, n_{1i}}).\end{gathered} \qquad (5)$$

Наприклад, з урахуванням [1, 16] при $n_1 = 5$, $n_{11} = 7$; $n_{12} = 6$; $n_{13} = 4$; $n_{14} = 2$; $n_{15} = 1$ $(i = \overline{1,5})$ на основі (5) $\mathbf{S}$ представимо як:

$$\begin{gathered}\mathbf{S} = \{\bigcup_{i=1}^{5} \{\bigcup_{j=1}^{n_{1i}} S_{ij}\}\} = \{\{S_{11}, S_{12}, S_{13}, S_{14}, S_{15}, S_{16}, S_{17}\}, \{S_{21}, S_{22}, S_{23}, S_{24}, S_{25}, S_{26}\}, \{S_{31}, S_{32}, S_{33}, S_{34}\}, \{S_{41}, S_{42}\}, \{S_{51}\}\} = \\ \{\{"11","12","13","14", 15","16","17"\},\{"21","22","23","24","25","26"\},\{"31","32","33","34"\}, \\ \{"41","42"\},\{"51"\}\} = \{\{"Енергетичний сектор", "Сектор хімічної промисловості", "Транспортний сектор", "Сектор інформаційно-телекомунікаційних технологій", "Сектор електронної телекомунікації", "Банківський сектор", "Фінансовий сектор"\},\{"Сектор централізованого водопостачання та водовідведення", "Сектор постачання електричної енергії", "Сектор постачання газу", "Сектор продуктів харчування", "Сектор сільського господарства", "Сектор охорони здоров'я"\},\{"Сектор комунальних послуг", "Сектор аварійних служб", "Сектор рятувальних служб", "Сектор служби екстреної допомоги населенню"\},\{"Сектор економіки", "Сектор безпеки держави"\}, \{"Сектор потенційно небезпечних технологій і виробництва"\}\},\end{gathered} \qquad (6)$$

де S_{11} = "11" = "Енергетичний сектор", S_{12} = "12" = "Сектор хімічної промисловості", …, S_{26} = "26" = "Сектор охорони здоров'я", …, S_{42} = "42" = "Сектор безпеки держави", а S_{51} = "51" = "Сектор потенційно небезпечних технологій і виробництв". Слід зазначити, що ідентифікатори секторів можуть бути цифрові або лінгвістичні, наприклад, для S_{41} це може відповідно бути "41" або "Сектор економіки".

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

$$\mathbf{U} = \{\bigcup_{i=1}^{n_2} U_i\} = \{U_1, U_2, ..., U_{n_2}\} = \{"01", "02", "03", \ldots, "n_2"\}, \quad (7)$$

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

Відповідно до [12] в Україні наявні 24 області, Автономна Республіка Крим, місто з особливим статусом Севастополь і столиця України – місто Київ, 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 (7) набере вигляду:

$$\mathbf{U} = \{\bigcup_{i=1}^{27} U_i\} = \{U_1, U_2, ..., U_{26}, U_{27}\} = \{"01", "02", \ldots, "26", "27"\} = \{"Автономна Республіка Крим"\}, \{Вінницька область"\}, \ldots, \{"м. Київ"\}, \{"м. Севастополь"\}, \quad (8)$$

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

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

$$\mathbf{O} = \{\bigcup_{i=1}^{n_3} O_i\} = \{O_1, O_2, ..., O_{n_3}\}, \quad (9)$$

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 (9) матиме вигляд:

$$\mathbf{O} = \{\bigcup_{i=1}^{3} O_i\} = \{O_1, O_2, O_3\} = \{"Д", "К", "П"\} = \{"1", "2", "3"\}, \quad (10)$$

де O_1 = "*Д*" = "1", O_2 = "*К*" = "2", а O_3 = "*П*" = "3".

Черговий компонент **N** – множина назв та унікальних ідентифікаційних номерів юридичної особи в ЄДРПОУ організацій-власників/розпорядників ІТС як ОКІ визначається виразом:

$$\mathbf{N} = \{\bigcup_{i=1}^{n_4} N_i\} = \{N_1, N_2, ..., N_{n_4}\}, \quad (11)$$

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

Наприклад, при $n_4 = 5$ $(i = \overline{1, 5})$ формулу (11) можна представити як:

$$\mathbf{N} = \{\bigcup_{i=1}^{5} N_i\} = \{N_1, N_2, N_3, N_4, N_5\} = \{"14360570", "00032129", "00039019", "23697280", "14305909"\} = \{"Приват банк", "Ощадбанк", "Укрсоцбанк", "Укргазбанк", "Райффайзен банк аваль"\} = \{"https://privatbank.ua", "https://www.oschadbank.ua", "https:// www.ukrsotsbank.com", "https://www.ukrgasbank.com", "https://aval.ua"\}. \quad (12)$$

Слід зазначити, що множина назв та унікальних ідентифікаційних номерів юридичної особи може відображатися у цифровому або лінгвістичному вигляді як ідентифікатор організації (підприємства, установи) з гіперпосиланням на офіційний веб-сайт.

П'ятий компонент **R** – множина реєстраційних номерів документів (за державним реєстром Держспецзв'язку, НБУ, тощо), що засвідчують наявність атестованих/ліцензованих систем чи засобів захисту інформації (наприклад, атестатів відповідності на КСЗІ, КЗЗІ, СУІБ або експертних висновків на засоби ТЗІ чи на ОТР КСЗІ в ІТС) та інші, яка відображається виразом:

$$\mathbf{R} = \{\bigcup_{i=1}^{n_5} R_i\} = \{R_1, R_2, ..., R_{n_5}\}, \quad (13)$$

де $R_i \subseteq \mathbf{R}$ $(i = \overline{1, n_5})$ – *i*-й реєстраційний номер документу, а n_5 їх кількість.

Наприклад, при $n_6 = 3 \quad (i = \overline{1,3})$ формула (13) матиме вигляд:

$$\mathbf{R} = \{\bigcup_{i=1}^{3} R_i\} = \{R_1,\ R_2, R_3\} = \{\text{"17589"}, \text{"12563"} , \text{"12569"} \}, \tag{14}$$

де R_1 = "17589", R_2 = "12563" та R_3 = "12569" – номери за реєстром Держспецзв'язку.

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

$$\mathbf{I} = \{\bigcup_{i=1}^{n_6} I_i\} = \{I_1 , I_2 , ..., I_{n_6}\}, \tag{15}$$

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

Наприклад, при $n_6 = 4 \quad (i = \overline{1,4})$ з урахуванням [6, 13] формула (15) матиме вигляд:

$$\mathbf{I} = \{\bigcup_{i=1}^{4} I_i\} = \{I_1,\ I_2, I_3, I_4\} = \{\text{"}ВІ\text{"}, \text{"}КІ\text{"}, \text{"}СІ\text{"} , \text{"}ТІ\text{"} \} = \{\text{"01"}, \text{"02"}, \text{"03"}, \text{"04"}\}, \tag{16}$$

де I_1="*ВІ*"="02", I_2 ="*КІ*"="02", I_3="*СІ*"="03" та I_4 ="*ТІ*"="04".

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

$$\mathbf{C} = \{\bigcup_{i=1}^{n_7} C_i\} = \{C_1 , C_2 , ..., C_{n_7}\}, \tag{17}$$

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

Наприклад, при $n_7 = 10 \quad (i = \overline{1,10})$ з урахуванням [2, 5, 14-16] формула (17) матиме вигляд:

$$\mathbf{C} = \{\bigcup_{i=1}^{10} C_i\} = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10}\} = \{\text{"01"}, \text{"02"}, \text{"03"},\text{"04"},\text{"05"},\text{"06"},\text{"07"},\text{"08"},\text{"09"},\text{"10"}\} = \{\text{"Виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону)", "Негативний вплив на стан енергетичної безпеки держави (регіону)", "Негативний вплив на стан економічної безпеки держави", "Негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі", "Негативний вплив на систему управління державою", "Негативний вплив на суспільно-політичну ситуацію в державі", "Негативний вплив на імідж держави", "Порушення сталого функціонування фінансової системи держави", "Порушення сталого функціонування транспортної інфраструктури держави (регіону)", "Порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав"}, \tag{18}$$

де C_1 = "01" = "Виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону)", C_2 = "02" = "Негативний вплив на стан енергетичної безпеки держави (регіону)",…, а C_{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:

$$\mathbf{M} = \{\bigcup_{i=1}^{n_8} M_i\} = \{M_1 , M_2 , ..., M_{n_8}\}, \tag{19}$$

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

Наприклад, при $n_8 = 3 \quad (i = \overline{1,3})$ формула (19) набуде вигляду:

$$\mathbf{M} = \{\bigcup_{i=1}^{3} M_i\} = \{M_1, M_2, M_3\} = \{\text{"}GM\text{"},\text{"}MM\text{"},\text{"}YM\text{"}\} = \{\text{"1"},\text{"2"},\text{"3"}\}, \tag{20}$$

де M_1="*GM*"="1" = Google Maps, M_2 ="*MM*"="2" = Maps.Me, а M_3 ="*YM*"="3" = Yandex Maps.

В табл. 1 приведене умовне позначення семантики класифікатора ОКІІ держави, яке можна відобразити, як SS – UU – O – NN…N – RR…R – II – CC – MM.

Для приклада розглянемо побудову семантичної структури класифікатора Державної фіскальної служби (ДФС) України як ОКІІ, що відображається у вигляді представленому в табл. 2.

Таблиця 1

Семантика класифікатора ОКІІ держави

Елемент кортежу	**S** $(j=\overline{1,n_{1i}})$	**U**	**O**	**N**	**R**	**I**	**C**	**M**
i	$\overline{1,5}$	$\overline{1,27}$	$\overline{1,3}$	$\overline{1,n_4}$	$\overline{1,n_5}$	$\overline{1,3}$	$\overline{1,10}$	$\overline{1,3}$
Елемент множини	*SS*	*UU*	*O*	*NN…N*	*RR…R*	*II*	*CC*	*M*

Таблиця 2

Приклад класифікатора ОКІІ – ДФС України

Елемент кортежу	**S** $(j=7)$	**U**	**O**	**N**	**R**	**I**	**C**	**M**
i	1	26	1	39292197	14273	2	8	1
Елемент множини	17	26	1	39292197 (ДФС – http://sfs.gov.ua)	14273	03	08	1

Тобто, **17–26–1–39292197–14273–03–08–1**, де **S** $\supseteq S_{17}$ = "17" – фінансовий сектор, **U** $\supseteq U_{26}$ = "26" – місто Київ, **O** $\supseteq O_1$ = "*Д*" = "1" – державна форма власності, **N** $\supseteq N_1$ = 39292197 – універсальний ідентифікуючий номер ЄДРПОУ "ДФС" (http://sfs.gov.ua), **R** $\supseteq R_1$ = 14273 – номер атестату відповідності на КСЗІ ІТС центру сертифікації ключів Інформаційно-довідкового департаменту ДФС, за реєстром Держспецзв'язку, **I** $\supseteq I_2$ = "*СІ*" = "03" – службова інформація, **C** $\supseteq C_8$ = "08" – порушення сталого функціонування фінансової системи держави, **M** $\supseteq M_1$ = "*GM*" = "1" – ресурс Google Maps.

На рис. показано приклад можливого відображення елементу множини **M**.

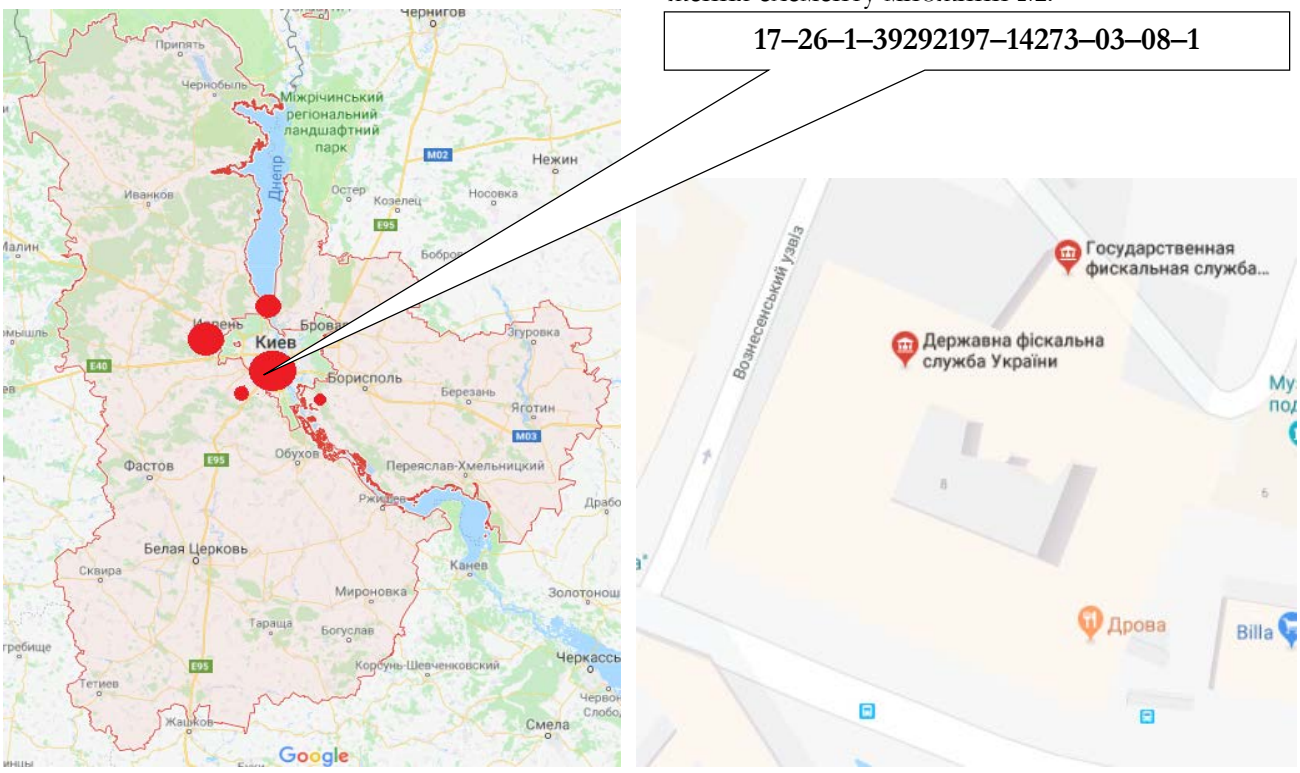

Рис. Приклад відображення M_1 = "*GM*" – зображення місця знаходження ДФС України

Висновок. У даному дослідженні запропоновано базову кортежну модель класифікатора ОКІІ держави, яка за рахунок множин ідентифікаторів секторів, адміністративно-територіальних одиниць України, форм власності, назв організацій, видів інформації, реєстраційних номерів документів, ідентифікаторів негативних наслідків кібератак на ІТС, ідентифікаторів геолокаційних ресурсів за місцем знаходження КІ, введених у кортеж дає змогу побудувати класифікатор та відобразити його у семантичному вигляді для подальшого створення практичного механізму формування переліку ІТС ОКІІ України.

ЛІТЕРАТУРА

[1]. "Про основні засади забезпечення кібербезпеки України" Верховна Рада України, Закон України від 05.10.2017 р. [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*, pp. 397-402, 2017.

[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 на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", *Захист інформації*, Т. 19, № 3, С. 214-222, 2017.

[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, 2014, 332 с., 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, С. 185, 2017.

[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- no 32- vid- 28022017- prezydentu-ukrayiny- shchodo- rishennya- rnbo- vid- 29122016-pro-zagrozy.

[9]. С. Гнатюк, В. Сидоренко, Н. Сейлова, "Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави", *Безпека інформації*, Том 23, № 2, С. 87-91, 2017.

[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 Держспецзв'язку, Наказ № 93 від 16.03.2007 [Електронний ресурс]. Режим доступу: http://zakon0.rada.gov.ua/laws/show/z0820-07.

[12]. Регіони України. [Електронний ресурс]. Режим доступу: 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.

[14]. О. Корченко, Ю. Дрейс, О. Романенко "Критична інформаційна інфраструктура України: терміни, сектори і наслідки", *Захист інформації*, Т. 19, № 4, С.303-309, 2017.

[15]. О. Корченко, Ю. Дрейс, О. Романенко "Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури", *Актуальні проблеми забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції* (Закарпатська область, Міжгірський район, село Верхнє Студене, 21-24 лютого 2018 р.), К: Видавництво Європейського університету, С. 81-86, 2018.

[16]. Y. Dreys, M. Roshchuk, O. Romanenko, "Sectors of Critical Informational Infrastructure", *Актуальні проблеми забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції* (Закарпатська область, Міжгірський район, село Верхнє Студене, 21-24 лютого 2018 р.), К: Видавництво Європейського університету, С.141-143, 2018.

МОДЕЛЬ КЛАССИФИКАТОРА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

Автоматизация процессов предоставления услуг во всех сферах обеспечения жизнедеятельности человека, общества и государства привела к ужесточению требований к защите информации в информационно-телекоммуникационных системах (ИТС) потенциально опасных объектов критической инфраструктуры. Согласно существующего нормативно-правового обеспечения, связанного с объектами критической инфраструктуры, прослеживается неполнота относительно возможности их корректной классификации, а также не сформирован перечень ИТС таких объектов и отсутствуют критерии оценивания негативных последствий от кибератак. Решение указанных вопросов позволит сформировать такой классификатор объектов критической информационной инфраструктуры, который даст возможность создать условия для повышения их устойчивости к кибератакам. В соответствии с этим предлагается средство классификации объектов критической информационной инфраструктуры. В

основу его построения заложена кортежных модель, составляющими которой являются упорядоченные идентификаторы объектов критической инфраструктуры, которые включают: сектор критической информационной инфраструктуры государства; административно-территориальную единицу Украины; название или идентификационный номер юридического лица; форму собственности организации-владельца/распорядителя ИТС; вид информации, обрабатываемой в ИТС; регистрационные номера документов, удостоверяющих наличие аттестованных/лицензированных систем или средств защиты информации; негативные последствия от кибератак на ИТС. С помощью предложенной модели представлены примеры классификации объектов критической информационной инфраструктуры государства, а в дальнейшем она позволит сформировать перечень соответствующих ИТС для обеспечения их первоочередной защиты от кибератак.
Ключевые слова: информационно-телекоммуникационная система, кибератака, критическая информационная инфраструктура, классификатор объектов, кортежная модель, негативные последствия.

THE MODEL OF OBJECTS CLASSIFIER OF CRITICAL INFORMATION INFRASTRUCTURE OF THE STATE

Providing the process automation services in all spheres of human, society and state life support has led to increased demands for the information protection in information and telecommunication systems (ITS) of potentially dangerous objects of critical infrastructure of the state. In accordance with the existing legal and regulatory framework related to the objects of critical infrastructure, there is an incompleteness regarding the possibility of their proper classification, there is also no list of ITS of such objects and there are no criteria for the negative consequences assessment. Solving these issues will generate the formation of such objects classifier of critical information infrastructure, which will enable the creation of conditions to increase their resilience to cyber attacks. Accordingly, a tool is proposed for classifying objects of critical information infrastructure. The basis of its construction is a tuple model, the components of which are ordered identifiers of critical infrastructure objects that reflect: the sector of the critical information infrastructure of the state; administrative territorial unit of Ukraine; name or identification number of the legal entity; form of ownership of the organization-owner / manager of ITS; the type of information processed in the ITS; registration numbers of documents certifying the availability of certified/licensed systems or information security means; the negative consequences of cyber attacks on ITS. With the help of the proposed model, examples of objects classification of critical information infrastructure of the state are presented, and it will give an opportunity to form a list of relevant ITS to ensure their priority protection against cyber attacks in future.
Keywords: information-telecommunication system, cyberattack, critical information infrastructure, classifier objects, basic model, negative consequences.

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.
E-mail: icaocentre@nau.edu.ua.
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.
Korchenko Alexander, 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.

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри інноваційних технологій професійної освіти Національного авіаційного університету.
E-mail: y.dreis@nau.edu.ua.
Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой инновационных технологий профессионального образования Национального авиационного университета.
Yurii Dreis, PhD in Eng. (Information security), Associate Professor, Head of the Innovative Technologies Professional Education Department, National Aviation University (Kyiv, Ukraine).

Романенко Ольга Олександрівна, студентка кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
E-mail: olya_olek@ukr.net.
Романенко Ольга Александровна, студентка кафедры компьютеризированных систем защиты информации Национального авиационного университета.
Olga Romanenko, Student of the Academic Department of Computerized Information Security Systems, National Aviation University.

Бичков Володимир Вячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університета.
E-mail: bychkov.volodymyr@gmail.com.
Бычков Владимир Вячеславович, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.
Bychkov Volodymyr, senior lecturer of IT-Security Academic Department, National Aviation University.