© Korchenko A., Dreis Yu., Roshchuk M., Romanenko O. Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 29-35.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.24.12606

МОДЕЛЬ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ ВІД КІБЕРАТАК НА КРИТИЧНУ ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ ДЕРЖАВИ

Олександр Корченко, Юрій Дрейс, Рощук Марія, Ольга Романенко

Національний авіаційний університет, Україна

КОРЧЕНКО Олександр Григорович, д.т.н.

Рік та 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, візит-професор Університету в Бельсько-Бялій (Гуманітарно-технічна академія в Бельсько-Бялій, м. Бельсько-Бяла, Польща), провідний науковий співробітник Національної академії СБ України.
Наукові інтереси: інформаційна та авіаційна безпека.
Публікації: більше 350 наукових публікацій, серед яких монографії, словники, навчальні посібники, підручники, статті, патенти та авторські свідоцтва на винаходи.
E-mail: icaocentre@nau.edu.ua

ДРЕЙС Юрій Олександрович, к.т.н.

Рік та місце народження: 1984 рік, смт. Червоноармійськ, Житомирська область, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова, 2007 рік.
Посада: завідувач кафедри інноваційних технологій професійної освіти з 2016 року.
Наукові інтереси: охорона державної таємниці, захист інформації з обмеженим доступом, критична інформаційна інфраструктура.
Публікації: більше 85 наукових публікацій, серед яких підручник, навчальні посібники, методичні рекомендації, наукові статті та авторські свідоцтва на комп'ютерні програми.
E-mail: y.dreis@nau.edu.ua

РОЩУК Марія Василівна

Рік та місце народження: 1994 р., с. Ясенів Пільний, Івано-Франківська обл., Україна.
Освіта: Національний авіаційний університет, 2016 р.
Посада: аспірант Національного авіаційного університету з 2016 р.
Наукові інтереси: інформаційне право, електронне урядування.
Публікації: 20 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: Roshchukmv@gmail.com

РОМАНЕНКО Ольга Олександрівна

Рік та місце народження: 1996 рік, с. Тайки, Ємільчинський район, Житомирська область, Україна.
Освіта: Вінницький національний технічний університет, 2017 рік.
Посада: фахівець кафедри інноваційних технологій професійної освіти з 2017 року.
Наукові інтереси: інформаційна безпека, захист інформації, охорона державної таємниці.
Публікації: більше 10 наукових публікацій, серед яких розділ в монографії, статті, матеріали і тези доповідей та авторські свідоцтва.
E-mail: olya_olek@ukr.net

Анотація. *Провідні держави світу приділяють велику увагу кіберзахисту критичної інфраструктури. Не є виключенням Україна, яка має об'єкти критичної інфраструктури в яких міститься інформація, що становить державну таємницю (ДТ). Широке використання сучасних інформаційно-телекомунікаційних технологій в об'єктах критичної інфраструктури створює низку нових уразливостей та потенційних загроз, тому є необхідність оцінювати негативні наслідки національній безпеці у разі витоку ДТ. Відомі підходи дозволяють визначати шкоду від розголошення чи втрати ДТ в бальному еквіваленті і грошовому але тільки для одного суб'єкта режимно-секретної діяльності. Тому залишається не вирішеним питання оцінювання для множини відповідних об'єктах в межах визначених областей чи для держави в цілому. З огляду на це, розроблено модель оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави, яка за рахунок визначених множин потенційних порушень, типових загроз, ступенів секретності, зводу відомостей, що становлять державну таємниці, показників економічної шкоди, тяжких наслідків та інших (що входять до відповідного кортежу), і дає можливість створити метод оцінювання негативних наслідків витоку ДТ, як в межах окремих областей, так і для держави в цілому.*

Ключові слова: *державна таємниця, модель, кібератака, інформаційно-телекомунікаційна система, критична інфраструктура, державний експерт, суб'єкт режимно-секретної діяльності, оцінювання наслідків.*

Вступ

Відомо, що до критичної інфраструктури належать об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної та економічної сфери держави та негативно вплине на рівень її обороноздатності та національної безпеки [1]. Критична інфраструктура України має такі об'єкти, системи і ресурси, які містять ДТ, втрата або розголошення якої нанесе негативний вплив на людину, суспільство та державу. В Україні відсутні методи та способи оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру. Разом з тим існують законодавчі вимоги [2] для державного експерта з питань таємниць щодо необхідності розробки критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації. У зв'язку з цим, необхідність створення практичного механізму визначення такої шкоди або негативних наслідків витоку ДТ є актуальною науковою задачею.

Аналіз досліджень

На даний час до офіційного документу державного експерта з питань таємниць щодо визначення величини можливої шкоди при віднесенні інформації до ДТ відносять [3], недоліком якого є представлення цієї шкоди у бальному еквіваленті. Також існує єдиний метод оцінювання шкоди національній безпеці України у разі витоку ДТ, який висвітлено у [4], який розраховує величину нанесеної шкоду, як у бальному, так і в грошовому еквіваленті, але при розголошенні секретної інформації або втрати її матеріальних носіїв на одному суб'єкті режимно-секретної діяльності.

Метою даної роботи є розробка моделі оцінювання наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави, яка дасть можливість створити метод оцінювання негативних наслідків (шкоди) витоку ДТ від кібератак на об'єкти критичної інформаційної інфраструктури, як в межах окремих областей (в т.ч. й тимчасово окупованих територій), так і для держави в цілому.

Основна частина дослідження

Виходячи з актуальності, пропонується модель оцінювання наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави, яка містить основні параметри для оцінювання шкоди, представлених у вигляді кортежу:

$$\mathbf{IDN} = < \mathbf{IDN_1}, \mathbf{IDN_2}, ..., \mathbf{IDN_i}, ..., \mathbf{IDN_m} >, \quad (1)$$

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

Наприклад, з урахуванням [2-14] відповідно до існуючої упорядкованої послідовності параметрів звіту про стан забезпечення охорони ДТ (ОДТ) та узагальненого звіту про стан забезпечення ОДТ за підзвітні суб'єкти режимно-секретної діяльності (СРСД) [11], при *m* = 13 кортеж (1) сформується як:

$$\mathbf{IDN} = < \mathbf{IDN_1}, \mathbf{IDN_2}, ..., \mathbf{IDN_7}, ..., \mathbf{IDN_{13}} > = < \mathbf{U}, \mathbf{N}, \mathbf{V}, \mathbf{T}, \mathbf{D}, \mathbf{DS}, \mathbf{TS}, \mathbf{M}, \mathbf{OB}, \mathbf{CP}, \mathbf{ED}, \mathbf{H}, \mathbf{LC} >, \quad (2)$$

де $\mathbf{IDN_1} = \mathbf{U}$ (множина ідентифікаторів адміністративно-територіальних одиниць (*Units*) України, в межах якої знаходиться об'єкт критичної інфраструктури (ОКІ) – СРСД); $\mathbf{IDN_2} = \mathbf{N}$ (множина назв

або/та унікальних ідентифікаційних номерів (*Number*) юридичної особи в Єдиному державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників/розпорядників інформаційно-телекомунікаційної системи (ІТС) як об'єкта критичної інформаційної інфраструктури (ОКІІ)); $\mathbf{IDN_3} = \mathbf{V}$ (множина потенційних порушень (*Violation*), які кваліфікують відповідні підмножини типових загроз у сфері ОДТ, що є підставою для оцінювання наслідків (шкоди); $\mathbf{IDN_4} = \mathbf{T}$ (множина типових загроз (*Threat*) у сфері ОДТ); $\mathbf{IDN_5} = \mathbf{D}$ (множина відомостей (*Data*) у вигляді номера статті зводу відомостей, що становить ДТ (ЗВДТ) **V**); $\mathbf{IDN_6} = \mathbf{DS}$ (множина ступенів секретності (СС) (*Degree of Secrecy*) для **D**); $\mathbf{IDN_7} = \mathbf{TS}$ (множина завдань (*Task*) з ОДТ); $\mathbf{IDN_8} = \mathbf{M}$ (множина заходів (засобів і способів) (*Method*) з усунення (нейтралізації) загроз захищеності для **D**); $\mathbf{IDN_9} = \mathbf{OB}$ (множина об'єктів (*Objects*) для **D**); $\mathbf{IDN_{10}} = \mathbf{CP}$ (множина складових частин об'єктів (СЧО) (*Component Parts of objects*) для **D**); $\mathbf{IDN_{11}} = \mathbf{ED}$ (множина показників економічної шкоди (*Economic Damage*)); $\mathbf{IDN_{12}} = \mathbf{H}$ (множина показників інших тяжких наслідків (*other Hard consequences*)); $\mathbf{IDN_{13}} = \mathbf{LC}$ (множина ідентифікаторів рівня класифікації терористичних загроз (*Lever of Classification of terrorist threats*)).

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

$$\mathbf{U} = \{\bigcup_{i=1}^{m_1} U_i\} = \{U_1, U_2, ..., U_{m_1}\}, \quad (3)$$

де $U_i \subseteq \mathbf{U}$ $(i = \overline{1, m_1})$ – *i*-й ідентифікатор адміністративно-територіальної одиниці, а m_1 їх кількість.

В Україні наявні 24 області, Автономна Республіка Крим, місто з особливим статусом Севастополь і столиця України – місто Київ, тому ідентифікатори адміністративно-територіальних одиниць можуть бути цифрові або лінгвістичні.

Наприклад, при $m_1 = 27$ $(i = \overline{1, 27})$ формула (3) набуде вигляду [5-7]:

$$\mathbf{U} = \{\bigcup_{i=1}^{27} U_i\} = \{U_1, U_2, ..., U_{26}, U_{27}\}, \quad (4)$$

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

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

$$\mathbf{N} = \{\bigcup_{i=1}^{m_2} N_i\} = \{N_1, N_2, ..., N_{m_2}\}, \quad (5)$$

де $N_i \subseteq \mathbf{N}$ $(i = \overline{1, m_2})$ – *i*-а назва СРСД та/або номер ЄДРПОУ організації (підприємства, установи), а m_2 їх кількість.

Наприклад, при $m_2 = 3$ $(i = \overline{1, 3})$ формулу (5) можна представити як [5-7, 14]:

$$\mathbf{N} = \{\bigcup_{i=1}^{3} N_i\} = \{N_1, N_2, N_3\}, \quad (6)$$

де N_1 = {«A2299»} = {«08385264»} = військова частина (в/ч) м. Бровари, N_2 = {«A4036»} = {«08025979»} = в/ч м. Дніпро, а N_3 = {«A2253»} = {«143217652»} = в/ч м. Чернігів.

Наступний компонент **V** – множина потенційних порушень, які кваліфікують відповідні підмножини типових загроз у сфері ОДТ, що є підставою для оцінювання наслідків (шкоди) набуде вигляду:

$$\mathbf{V} = \{\bigcup_{i=1}^{m_3} V_i\} = \{V_1, V_2, ..., V_{m_3}\}, \quad (7)$$

де $V_i \subseteq \mathbf{V}$ $(i = \overline{1, m_3})$ – *i*-а підмножина потенційних порушень, а m_3 їх кількість.

Наприклад, з урахуванням [2, 8] при m_3 =3 $(i = \overline{1, 3})$ формула (7) матиме вигляд:

$$\mathbf{V} = \{\bigcup_{i=1}^{3} V_i\} = \{V_1, V_2, V_3\}, \quad (8)$$

де V_1 = «Розголошення ДТ» [8, стаття 328], V_2 = «Втрата документів, що містять ДТ» [8, стаття 329], а V_3 = «Витік інформації, що становить ДТ» [8, статті 361-362].

Наступний компонент **T** – множина типових загроз у сфері ОДТ відображається як:

$$\mathbf{T} = \{\bigcup_{i=1}^{m_4} T_i\} = \{T_1, T_2, ..., T_{m_4}\}, \quad (9)$$

де $T_i \subseteq \mathbf{T}$ $(i = \overline{1, m_4})$ – *i*-а типова загроза, а m_4 кількість загроз.

Наприклад, з урахуванням [4, 9] при m_4= 6 $(i = \overline{1, 6})$ формула (9) визначається як:

$$\mathbf{T} = \{\bigcup_{i=1}^{6} T_i\} = \{T_1, T_2, T_3, T_4, T_5, T_6\}, \quad (10)$$

де T_1 = «Несанкціоноване отримання секретної інформації зацікавленими особами у результаті порушення правил секретного діловодства і порядку допуску та доступу до матеріальних носів секретної інформації», T_2 = «Отримання секретної інформації іноземними спецслужбами у результаті агентурного проникнення (шпигунство)», T_3 = «Розголошення відомостей, що становлять ДТ», T_4 = «Втрата матеріальних носіїв секретної інформації», T_5 = «Перехоплення секретної інформації, яка передається за допомогою засобів телекомунікації (ІТС, АС тощо), а також технічними каналами витоку інформації, в тому числі каналами побічного електромагнітного випромінювання і наводок (ПЕМВН), зокрема в мережах електроживлення технічних засобів обробки і збереження інформації», T_6 = «Знищення або модифікація секретної інформації деструктивними силовими впливами».

Наступний компонент **D** – множина відомостей у вигляді номера статті ЗВДТ щодо **V**, сформовано як:

$$\mathbf{D} = \{\bigcup_{i=1}^{m_5} \mathbf{D}_i\} = \{\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_{m_5}\}, \quad (11)$$

де $\mathbf{D}_i \subseteq \mathbf{D}$ $(i = \overline{1, m_5})$ – підмножина *i*-ї сфери (класи) відомостей, що становлять ДТ, а m_5 їх кількість.

Наприклад, при $m_5 = 4$ підмножина $\mathbf{D_i}$ матиме вигляд [2, 10]:

$$\mathbf{D} = \{\bigcup_{i=1}^{4} \mathbf{D}_i\} = \{\mathbf{D}_1, \mathbf{D}_2, \mathbf{D}_3, \mathbf{D}_4\}, \quad (12)$$

де $\mathbf{D}_1$ = «**Сфера оборони**», $\mathbf{D}_2$ = «**Сфера економіки, науки і техніки**», $\mathbf{D}_3$ = «**Сфера зовнішніх відносин**», $\mathbf{D}_4$ = «**Сфера державної безпеки та охорони правопорядку**».

Підмножину $\mathbf{D}_i$ наведено як:

$$\mathbf{D}_i = \{\bigcup_{j=1}^{m_{5i}} \mathbf{D}_{ij}\} = \{\mathbf{D}_{i1}, \mathbf{D}_{i2}, ..., \mathbf{D}_{im_{5i}}\}, \quad (13)$$

де $\mathbf{D}_{ij} \subseteq \mathbf{D}_i$ $(j = \overline{1, m_{5i}})$ – *j*-а підмножина груп відомостей споріднених за певною темою чи близьких за певними характеристиками до об'єкта ДТ у межах підмножини *i*-ї сфери, а m_{5i} кількість груп *i*-ї підмножини.

Підмножину $\mathbf{D}_{ij}$ представлено як:

$$\mathbf{D}_{ij} = \{\bigcup_{k=1}^{m_{5ij}} D_{ijk}\} = \{D_{ij1}, D_{ij2}, ..., D_{ijm_{5ij}}\}, \quad (14)$$

де $D_{ijk} \subseteq \mathbf{D}_{ij}$ $(k = \overline{1, m_{5ij}})$ – *k*-а стаття відомостей, що становлять ДТ, яка входить до складу *j*-ї групи *i*-ї сфери, а m_{5ij} їх кількість.

З урахуванням (13) та (14) формула (11) визначається як:

$$\begin{gathered}\mathbf{D} = \{\bigcup_{i=1}^{m_5} \mathbf{D}_i\} = \{\bigcup_{i=1}^{m_5} \{\bigcup_{j=1}^{m_{5i}} \mathbf{D}_{ij}\}\} = \\ \{\bigcup_{i=1}^{m_5} \{\bigcup_{j=1}^{m_{5i}} \{\bigcup_{k=1}^{m_{5ij}} D_{ijk}\}\}\} = \\ \{\{D_{1.1.1}, D_{1.1.2}, ..., D_{1.1.m_{5.1.1}}\}, \{D_{1.2.1}, D_{1.2.2}, ..., D_{1.2.m_{5.1.2}}\}, ..., \\ \{D_{1.m_{5.1}.1}, D_{1.m_{5.1}.2}, ..., D_{1.m_{5.1}.m_{5.1.m_{5.1}}}\}, \\ \{D_{2.1.1}, D_{2.1.2}, ..., D_{2.1.m_{5.2.1}}\}, \{D_{2.2.1}, D_{2.2.2}, ..., D_{2.2.m_{5.2.2}}\}, ..., \\ \{D_{2.m_{5.2}.1}, D_{2.m_{5.2}.2}, ..., D_{2.m_{5.2}.m_{5.2.m_{5.2}}}\}, \\ ..., \\ \{D_{m_5.1.1}, D_{m_5.1.2}, ..., D_{m_5.1.m_{5.m_5.1}}\}, \{D_{m_5.2.1}, D_{m_5.2.2}, ..., D_{m_5.2.m_{5.m_5.2}}\}, ..., \\ \{D_{m_5.m_{5.m_5}.1}, D_{m_5.m_{5.m_5}.2}, ..., D_{m_5.m_{5.m_5}.m_{5.m_5.m_{5.m_5}}}\}\}, \\ (i = \overline{1, m_5},\ j = \overline{1, m_{5i}}, k = \overline{1, m_{5ij}}).\end{gathered} \quad (15)$$

Наприклад, відповідно до [10] при $m_5 = 4$ $(i = \overline{1,4})$, $m_{5.1} = 12$ $(j = \overline{1,12})$, $m_{5.1.1} = 12$ $(k = \overline{1,12})$, …, $m_{5.1.12} = 6$ $(k = \overline{1,6})$; $m_{5.2} = 7$ $(j = \overline{1,7})$, $m_{5.2.1} = 22$ $(k = \overline{1,22})$, …, $m_{5.2.7} = 8$ $(k = \overline{1,8})$; $m_{5.3} = 2$ $(j = \overline{1,2})$, $m_{5.3.1} = 7$ $(k = \overline{1,7})$, $m_{5.3.2} = 7$ $(k = \overline{1,7})$; $m_{5.4} = 12$ $(j = \overline{1,12})$, $m_{5.4.1} = 19$ $(k = \overline{1,19})$, …, $m_{5.4.12} = 5$ $(k = \overline{1,5})$ формула (11) матиме вигляд:

$$\begin{gathered}\mathbf{D} = \{\bigcup_{i=1}^{4} \{\bigcup_{j=1}^{m_{4i}} \{\bigcup_{k=1}^{m_{4ij}} D_{ijk}\}\}\} = \{\{\{D_{1.1.1}, ..., D_{1.1.12}\}, ..., \\ \{D_{1.12.1}, ..., D_{1.12.6}\}\}, \\ \{\{D_{2.1.1}, ..., D_{2.1.22}\}, ..., \{D_{2.7.1}, ..., D_{2.7.8}\}\}, \\ \{\{D_{3.1.1}, ..., D_{3.1.7}\}, \{D_{3.2.1}, ..., D_{3.2.7}\}\}, \\ \{D_{4.1.1}, ..., D_{4.1.9}\}, ..., \{D_{4.12.1}, ..., D_{4.12.5}\}\}\},\end{gathered} \quad (16)$$

де $D_{1.1.1}$ = «1.1.1» = «Відомості про стратегічне розгортання військ (сил)», …, $D_{1.1.12}$ = «1.1.12» = «Відомості про заходи, які плануються або провадяться для захисту від зброї масового ураження, володіння якими дає змогу зацікавленій стороні вплинути на їх ефективність», …, $D_{4.12.1}$ = «4.12.1» = «Відомості про зміст матеріалів дізнання (досудового слідства), якщо розголошення відомостей про це може завдати шкоди національним інтересам і безпеці. Рішення про необхідність засекречування та розсекречування (але не пізніше вступу в силу вироку суду) інформації приймає державний експерт з питань таємниць», …, $D_{4.15.5}$ = «4.12.5» = «Відомості, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення негласної слідчої (розшукової) дії, розголошення яких створює загрозу національним інтересам і безпеці».

Шостий компонент **DS** – множина СС для D визначається виразом:

$$\mathbf{DS} = \{\bigcup_{i=1}^{m_6} DS_i\} = \{DS_1, DS_2, ..., DS_{m_6}\}, \quad (17)$$

де $DS_i \subseteq \mathbf{DS}$ $(i = \overline{1, m_6})$ – *i*-а СС, а m_6 їх кількість.

Наприклад, при m_6 =3 $(i = \overline{1,3})$ з урахуванням [2, 8] формула (17) сформовано як:

$$\mathbf{DS} = \{\bigcup_{i=1}^{3} DS_i\} = \{DS_1, DS_2, DS_3\}, \quad (18)$$

де DS_1 = «Таємно (Т)», DS_2 = «Цілком таємно (ЦТ)», DS_3 = «Особливої важливості (ОВ)».

Наступний компонент **TS** – множина завдань з ОДТ визначається виразом:

$$\mathbf{TS} = \{\bigcup_{i=1}^{m_7} TS_i\} = \{TS_1, TS_2, ..., TS_{m_7}\}, \quad (19)$$

де $TS_i \subseteq \mathbf{TS}$ $(i = \overline{1, m_7})$ – *i*-е завдання з ОДТ, а m_7 їх кількість.

Наприклад, при m_7 =6 $(i = \overline{1,6})$ з урахуванням [9] формула (19) матиме вигляд:

$$\mathbf{TS} = \{\bigcup_{i=1}^{6} TS_i\} = \{TS_1, TS_2, TS_3, TS_4, TS_5, TS_6\}, \quad (20)$$

де TS_1 = «Унеможливлення несанкціонованого отримання секретної інформації», TS_2 = «Попередження розголошення секретної інформації», TS_3 = «Запобігання втратам матеріальних носіїв секретної інформації», TS_4 = «Запобігання агентурному проникненню до секретної інформації збоку іноземних

спецслужб», TS_5 = «Виключення можливостей перехоплення секретної інформації, яка передається за допомогою засобів телекомунікації, а також існує у ПЕМВН в межах електроживлення технічних засобів обробки і зберігання секретної інформації», TS_6 = «Недопущення знищення або модифікації деструктивними силовими впливами».

Восьмий компонент **M** – множина заходів (засобів і способів) з усунення (нейтралізації) загроз захищеності для **D** у сфері ОДТ має вигляд:

$$\mathbf{M} = \{\bigcup_{i=1}^{m_8} M_i\} = \{M_1, M_2, ..., M_{m_8}\}, \quad (21)$$

де $M_i \subseteq \mathbf{M}$ $(i = \overline{1, m_8})$ – i-й захід (засіб і спосіб), а m_8 їх кількість.

Наприклад, з урахуванням [9] при m_8 =47 $(i = \overline{1,47})$ визначимо:

$$\mathbf{M} = \{\bigcup_{i=1}^{47} M_i\} = \{M_1, M_2, ..., M_{47}\}, \quad (22)$$

де M_1 = «Обладнання приміщень для проведення робіт, пов'язаних з ДТ у відповідності з вимогами НД», M_2 = «Зберігання секретних документів та інших матеріальних носіїв секретної інформації у спеціальних сховищах», …, M_{47} = «Вживання заходів криптографічного захисту».

Наступний компонент **OB** – множина об'єктів для **D**, сформуємо виразом:

$$\mathbf{OB} = \{\bigcup_{i=1}^{m_9} \mathbf{OB}_i\} = \{\mathbf{OB}_1, \mathbf{OB}_2, ..., \mathbf{OB}_{m_9}\}, \quad (23)$$

де $\mathbf{OB}_i \subseteq \mathbf{OB}$ $(i = \overline{1, m_9})$ – підмножина об'єктів i-ї сфери для **D**, а m_9 їх кількість. Компонент **OB** може відображатись як у цифровому, так і в лінгвістичному вигляді.

Наприклад, при $m_9 = 3$ з урахуванням [3] підмножина $\mathbf{OB_i}$ представлено як:

$$\mathbf{OB} = \{\bigcup_{i=1}^{3} \mathbf{OB}_i\} = \{\mathbf{OB}_1, \mathbf{OB}_2, \mathbf{OB}_3\}, \quad (24)$$

де $\mathbf{OB}_1$ = «**Сфера оборони»**, $\mathbf{OB}_2$ = «**Сфера економіки»**, $\mathbf{OB}_3$ = «**Сфера державної безпеки**».

Підмножину $\mathbf{OB}_i$ визначимо як:

$$\mathbf{OB}_i = \{\bigcup_{j=1}^{m_{9i}} OB_{ij}\} = \{OB_{i1}, OB_{i2}, ..., OB_{im_{9i}}\}, \quad (25)$$

де $OB_{ij} \subseteq \mathbf{OB}_i$ $(j = \overline{1, m_{9i}})$ – j-й об'єкт i-ї сфери для **D**, а m_{9i} їх кількість. З урахуванням (25) вираз (23) можна представити у такому вигляді:

$$\begin{gathered}\mathbf{OB} = \{\bigcup_{i=1}^{m_9} \mathbf{OB}_i\} = \{\bigcup_{i=1}^{m_9} \{\bigcup_{j=1}^{m_{9i}} OB_{ij}\}\} = \\ \{\{OB_{11}, OB_{12}, ..., OB_{1m_{91}}\}, \\ \{OB_{21}, OB_{22}, OB_{23}, ..., OB_{2m_{92}}\}, ..., \\ \{OB_{m_91}, OB_{m_92}, OB_{m_93}, ..., OB_{m_9m_{9m_9}}\},\end{gathered} \quad (26)$$

Наприклад, при m_9 = 3 $(i = \overline{1,3})$, $m_{9.1}$ = 16 $(i = \overline{1,16})$, $m_{9.2}$ = 8 $(i = \overline{1,8})$, $m_{9.3}$ = 6 $(i = \overline{1,6})$ з урахуванням [3] формула (23) матиме вигляд:

$$\begin{gathered}\mathbf{OB} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_{9i}} OB_{ij}\}\} = \{\{OB_{1.1}, OB_{1.2}, ..., OB_{1.16}\}, \\ \{OB_{2.1}, OB_{2.2}, ..., OB_{2.8}\}, \{OB_{3.1}, OB_{3.2}, ..., OB_{3.6}\}\},\end{gathered} \quad (27)$$

де $OB_{1.1}$ = «Вид Збройних Сил», $OB_{1.2}$ = «Округ», …, $OB_{1.16}$ = «Картографічна продукція», $OB_{2.1}$ = «Мобілізаційні потужності створення державних матеріальних резервів: міністерством, відомством», $OB_{2.2}$ = «Мобілізаційні потужності створення державних матеріальних резервів: підприємством, установою, організацією», …, $OB_{2.8}$ = «Залізничні вузли», $OB_{3.1}$ = «Системи і комплекси урядового і спеціального зв'язку», $OB_{3.2}$ = «Державні шифри», …, $OB_{3.6}$ = «Технічні засоби охорони, сигналізації».

Наступний компонент **CP** – множина СЧО для **D** відображається як:

$$\mathbf{CP} = \{\bigcup_{i=1}^{m_{10}} CP_i\} = \{CP_1, CP_2, ..., CP_{m_{10}}\}, \quad (28)$$

де $CP_i \subseteq \mathbf{CP}$ $(i = \overline{1, m_{10}})$ – i-та СЧО для D, а m_{10} їх кількість.

Наприклад, при m_{10} =5 $(i = \overline{1,5})$ з урахуванням [10] формула (28) матиме вигляд:

$$\mathbf{CP} = \{\bigcup_{i=1}^{5} CP_i\} = \{CP_1, CP_2, CP_3, CP_4, CP_5\}, \quad (29)$$

де CP_1 = «За окремими складовими показниками», CP_2 = «За сукупністю всіх складових показників», CP_3 = «За окремими показниками», CP_4 = «За сукупністю всіх показників», CP_5 = «Об'єкт у цілому».

Наступний компонент **ED** – множина показників економічної шкоди відповідно до обсягу витрат її складових, визначається виразом:

$$\mathbf{ED} = \{\bigcup_{i=1}^{m_{11}} ED_i\} = \{ED_1, ED_2, ..., ED_{m_{11}}\}, \quad (30)$$

де $ED_i \subseteq \mathbf{ED}$ $(i = \overline{1, m_{11}})$ – i-й складовий показник економічної шкоди (як витрат на заходи забезпечення ОДТ), а m_{11} їх кількість. Складовий показник може відображатись як лінгвістично, так і в цифровому вигляді.

Наприклад, при m_{11}= 6 $(i = \overline{1,6})$ з урахуванням [11] формула (30) відображається як:

$$\mathbf{ED} = \{\bigcup_{i=1}^{6} ED_i\} = \{ED_1, ED_2, ED_3, ED_4, ED_5, ED_6\}, \quad (31)$$

де ED_1 = «На утримання штатних працівників РСО», ED_2 = «На розмір виплаченої компенсації громадянам у зв'язку з виконанням секретних робіт (без урахування працівників РСО)», ED_3 = «На матеріально-технічне забезпечення, а також на перевезення та пересилання матеріальних носіїв секретної інформації, їх фізичну охорону», ED_4 = «На виплату грошових надбавок державним експертам з пи-

тань таємниць та членам експертних комісій», ED_5 = «На технічний захист секретної інформації», ED_6 = «На криптографічний захист секретної інформації».

Наступний компонент **H** – множина складових показників інших тяжких наслідків сформовано як:

$$\mathbf{H} = \{\bigcup_{i=1}^{m_{12}} \mathbf{H}_i\} = \{\mathbf{H}_1, \mathbf{H}_2, ..., \mathbf{H}_{m_{12}}\}, \quad (32)$$

де $\mathbf{H}_i \subseteq \mathbf{H}$ $(i = \overline{1, m_{12}})$ – i-а категорія інших тяжких наслідків, а m_{12} їх кількість.

Підмножину $\mathbf{H}_i$ визначимо як:

$$\mathbf{H}_i = \{\bigcup_{j=1}^{m_{12i}} H_{ij}\} = \{H_{i1}, H_{i2}, ..., H_{im_{12i}}\}, \quad (33)$$

де $H_{ij} \subseteq \mathbf{H}_i$ $(j = \overline{1, m_{12i}})$ – j-й показник i-ї категорії інших тяжких наслідків, а m_{12i} їх кількість. З урахуванням (32) вираз (33) можна представити у такому вигляді:

$$\begin{aligned} \mathbf{H} = \{\bigcup_{i=1}^{m_{12}} \mathbf{H}_i\} = \{\bigcup_{i=1}^{m_{12}} \{\bigcup_{j=1}^{m_{12i}} H_{ij}\}\} = \\ \{\{H_{11}, H_{12}, ..., H_{1m_{121}}\}, \\ \{H_{21}, H_{22}, H_{23}, ..., H_{2m_{122}}\}, ..., \\ \{H_{m_{12}1}, H_{m_{12}2}, H_{m_{12}3}, ..., H_{m_{12}m_{12m_{12}}}\}. \end{aligned} \quad (34)$$

Наприклад, при m_{12} = 5 $(i = \overline{1,5})$, $m_{12.1}$ = 2 $(j = \overline{1,2})$, $m_{12.2}$ = 3 $(j = \overline{1,3})$, $m_{12.3}$ = $m_{12.4}$ = 6 $(j = \overline{1,6})$, $m_{12.5}$ = 4 $(j = \overline{1,4})$ з урахуванням [3] вираз (34) матиме вигляд:

$$\begin{aligned} \mathbf{H} = \{\bigcup_{i=1}^{5} \{\bigcup_{j=1}^{m_{12i}} H_{ij}\}\} = \{\{H_{11}, H_{12}\}, \{H_{21}, ..., H_{23}\}, \\ \{H_{31}, ..., H_{36}\}, \{H_{41}, ..., H_{46}\}, \{H_{51}, ..., H_{54}\}\}, \end{aligned} \quad (35)$$

де H_{11} = «Повний розрив дипломатичних відносин, що може призвести до озброєного нападу на Україну чи її союзників або воєнних дій», H_{12} = «Повний контроль державного шифрованого листування з боку іншої держави», H_{21} = «Розрив дипломатичних відносин з однією або з кількома розвиненими державами», …, H_{23} = «Загроза життю чи свободі особам, які виконують розвідувальні чи корнтррозвідувальні завдання», H_{31} = «Розрив дипломатичних відносин з іншими державами (державою)», …, H_{36} = «Часткове (до 30%) розкриття розвідувальних можливостей держави за кордоном», H_{41} = «Зрив укладення Україною міжнародного договору», …, H_{46} = «Розкриття сил чи засобів негласного оперативного контролю, що застосовуються державними органами для виконання оперативно-розшукової діяльності», H_{51} = «Зрив переговорів з питань озброєння-роззброєння», …, H_{54} = «НСД (проникнення) на об'єкти, де впроваджено режим спеціального допуску і охорони».

Останній компонент **LC** – множина ідентифікаторів рівня класифікації терористичних загроз, визначається виразом:

$$\mathbf{LC} = \{\bigcup_{i=1}^{m_{13}} LC_i\} = \{LC_1, LC_2, ..., LC_{m_{13}}\}, \quad (36)$$

де $LC_i \subseteq \mathbf{LC}$ $(i = \overline{1, m_{13}})$ – i-й ідентифікатор рівня класифікації терористичних загроз, а m_{13} їх кількість. Ідентифікатор може відображатись як лінгвістично, так і в цифровому вигляді.

Наприклад, при m_{13} =4 $(i = \overline{1,4})$ з урахуванням [12, 13] формула (36) відображається як:

$$\mathbf{LC} = \{\bigcup_{i=1}^{4} LC_i\} = \{LC_1, LC_2, LC_3, LC_4\}, \quad (37)$$

де LC_1 = «Сірий (можлива загроза)», LC_2 = «Синій (потенційна загроза)», LC_3 = «Жовтий (імовірна загроза)», LC_4 = «Червоний (реальна загроза)».

Висновки

У роботі розроблено модель оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави, яка за рахунок визначених множин потенційних порушень, типових загроз, ступенів секретності, ЗВДТ, показників економічної шкоди, тяжких наслідків та інших (що входять до відповідного кортежу), і дає можливість створити метод оцінювання негативних наслідків витоку ДТ, як в межах окремих областей, так і для держави в цілому.

Література

[1] Д. Бірюков, С. Кондратов, О. Суходоля, «Зелена книга з питань захисту критичної інфраструктури в Україні», К., 176 с., 2016. URL: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf.

[2] Про державну таємницю, Закон України Верховної Ради України від 10.03.1994. URL: http://zakon5.rada.gov.ua/laws/show/385512/ed19940121.

[3] Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності, Наказ №22 від 09.11.1998 р., Київ, Збірка, №8, С.4–14, 1998.

[4] О. Корченко, О. Архипов, Ю. Дрейс, «Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія», НА СБ України, К., 332 с., 2014.

[5] О. Корченко, Ю. Дрейс, О. Романенко, «Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури», тези доповідей учасників IV Міжнародної науково-практичної конференції 21-24 лютого 2018 р., К., с. 81-86, 2018.

[6] О. Корченко, Ю. Дрейс, О. Романенко, «Формування множини параметрів оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави», зб. тез доповідей наук.-практ. конф., 30 березня 2018, К., с. 309-311, 2018.

[7] О. Корченко, Ю. Дрейс, О. Романенко, «Модель класифікатора об'єктів критичної інформаційної інфраструктури держави», *Захист інформації*, т. 20, №1, с. 5-11, 2018.

[8] Кримінальний кодекс України, Верховної Ради України, від 05.04.2001 № 2341-III, URL: http://zakon2.rada.gov.ua/laws/show/2341-14.

[9] О. Архипов, І. Бородавко, В. Ворожко, Оцінювання ефективності системи охорони державної таємниці: монографія, НА СБ України, Київ, 63 с., 2007.

[10] Про затвердження зводу відомостей, що становлять державну таємницю, Наказ Служби безпеки України від 12.08.2005 №440.

[11] Про затвердження форм звітів про стан забезпечення охорони державної таємниці та інструкцій щодо порядку їх оформлення і подання, Наказ Служби безпеки України від 26 вересня 2015 року №630. URL: https://ssu.gov.ua/ua/pages/173.

[12] О. Корченко, Ю. Дрейс, «Додаткові критерії оцінювання шкоди, нанесеної розголошенням державної таємниці або втрати матеріальних носіїв секретної інформації за рівнем класифікації терористичних загроз», тези доповідей учасників II Міжнародної науково-практичної конференції, 24-27 лютого 2016 р., К., с. 90-91, 2016.

[13] Про затвердження Положення про єдину державну систему запобігання, редагування і припинення терористичних актів та мінімізації їх наслідків, Постанова Кабміну від 18.02.2016 №92.

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

УДК 004.056 (045)

Корченко А.Г., Дрейс Ю.А., Рощук М.В., Романенко О.А. Модель оценки последствий утечки государственной тайны от кибератак на критическую информационную инфраструктуру государства

Аннотация. *Ведущие государства мира уделяют большое внимание киберзащиты критической инфраструктуры. Не является исключением и Украина, которая имеет объекты критической инфраструктуры в которых содержится информация, составляющая государственную тайну (ГТ). Широкое использование современных информационно-телекоммуникационных технологий в объектах критической инфраструктуры создает ряд новых уязвимостей и потенциальных угроз, поэтому есть необходимость оценивать негативные последствия национальной безопасности в случае утечки ГТ. Известны подходы позволяют определять ущерб от разглашения или потери ГТ в бальном эквиваленте и денежном но только на одном субъекте режимно-секретной деятельности. Поэтому остается нерешенным вопрос оценки для множества соответствующих объектах в пределах определенных областей или для государства в целом. Учитывая это, разработана модель оценки негативных последствий утечки ГТ от кибератак на критическую информационную инфраструктуру государства, за счет определенных множеств потенциальных нарушений, типичных угроз, степеней секретности, свода сведений, составляющих государственную тайну, показателей экономического ущерба, тяжелых последствий и других (входящих в соответствующий кортежа), и дает возможность создать метод оценки негативных последствий утечки недели как в пределах отдельных областей, так и для государства в целом.*

Ключевые слова: *государственная тайна, модель, кибератака, информационно-телекоммуникационная система, критическая инфраструктура, государственный эксперт, субъект режимно-секретной деятельности, оценка последствий.*

Korchenko A., Dreis Yu., Roshchuk M., Romanenko O. Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state

Abstarct. *Today, more and more attention is paying on cybersecurity of critical information infrastructure by leading world state. Ukraine, which has critical infrastructure facilities in information and telecommunication systems of which the information that constitutes a state secret information, is not an exception. Extensive use of modern information and telecommunication technologies in critical infrastructure objects leading a lot of new vulnerabilities and potential cyberattacks. Therefore, the negative consequences for national security in case of a leak the state secret should be evaluated. Well-known approach allows to determine the damage from disclosure or loss of state secret in the score equivalent as well as monetary value, but only on one subject of regime-secret activity without taking into account the information and telecommunication system. Consequently, the question remains about the assessment of the negative consequences of the leakage of information with limited access from cyberattacks to information and telecommunication systems for a complex of critical infrastructure in a given rayon or for the state as a whole. In view of this, was developed the consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state which take into account the determined numerous of potential violation, typical threats, secrecy degree, a set of information constituting state secrets, indicators of economic damage, severe consequences and others (included in the corresponding list), affording to create the method of evaluating negative consequences of SS from cyberattacks to the critical information infrastructure of the state.*

Key words: *state secret, model, cyberattack, information-telecommunication system, critical infrastructure, state expert, subject of regime-secret activity, impact assessment.*

Отримано 20 *лютого 2018 року*, затверджено редколегією 20 *березня 2018 року*