МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

IX Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)

Електронна версія

Київ
2018

УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

УДК 004.056.5
Корченко О.Г.
доктор технічних наук, професор
Національна академія СБ України
Дрейс Ю.О.
кандидат технічних наук, доцент
Національний авіаційний університет
Романенко О.О.
Національний авіаційний університет

ФОРМУВАННЯ МНОЖИНИ ПАРАМЕТРІВ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ ВІД КІБЕРАТАК НА КРИТИЧНУ ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ ДЕРЖАВИ

З огляду на наявність в державі тимчасово окупованих територій та районів проведення антитерористичної операції, гостро постає питання щодо необхідності забезпечення захисту державних інформаційних ресурсів на об'єктах критичної інфраструктури (ОКІ), які є важливими для забезпечення національної безпеки України від терористичних загроз. Наразі основним завданням політики національної безпеки є захист державного суверенітету України, її територіальної цілісності, недоторканості державного кордону, що базується на принципі своєчасності й адекватності заходів захисту національних інтересів реальним і потенційним загрозам. В інформаційній сфері до таких загроз належить розголошення інформації, яка становить державну таємницю (ДТ), або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави. Тому оцінювання негативних наслідків (шкоди) витоку державної таємниці від кібератак на інформаційно-телекомунікаційні системи (ІТС) ОКІ є актуальним завданням.

Розроблено модель представлення параметрів шкоди у вигляді кортежу, при $m = 14$ визначимо як [1-5]:

$$\mathbf{IDN} = <\mathbf{IDN}_1, \mathbf{IDN}_2, \mathbf{IDN}_3, \mathbf{IDN}_4, \mathbf{IDN}_5, \mathbf{IDN}_6, \mathbf{IDN}_7, \mathbf{IDN}_8, \mathbf{IDN}_9, \mathbf{IDN}_{10}, \mathbf{IDN}_{12}, \mathbf{IDN}_{13}, \mathbf{IDN}_{14} > =$$
$$< \mathbf{U},\ \mathbf{N},\ \mathbf{E},\ \mathbf{A},\ \mathbf{D},\ \mathbf{DS},\ \mathbf{T},\ \mathbf{CS},\ \mathbf{CW},\ \mathbf{L},\ \mathbf{P},\ \mathbf{CA},\ \mathbf{TD},\ \mathbf{LCT} >,$$

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: 1) **U** – множина ідентифікаторів адміністративно-територіальних одиниць України, в межах якої знаходиться ОКІ – суб'єкт режимно-секретної діяльності (СРСД) і відображається як [1]: $\mathbf{U} = \{\bigcup_{i=1}^{m_1} U_i\} = \{U_1, ..., U_{m_1}\}$, де $U_i \subseteq \mathbf{U}$ $(i = \overline{1,m_1})$ – ідентифікатор адміністративно-територіальної одиниці, а m_1 їх кількість $(m_1 = 27)$; 2) **N** – множина назв або/та унікальних ідентифікаційних номерів юридичної особи в Єдиному

державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників / розпорядників ІТС як об'єкта критичної інформаційної інфраструктури, визначається виразом [1]: $\mathbf{N} = \{\bigcup_{i=1}^{m_2} N_i\} = \{N_1, ..., N_{m_2}\}$, де $N_i \subseteq \mathbf{N}$ $(i = \overline{1, m_2})$ – i-та назва СРСД та/або номер ЄДРПОУ організації (підприємства, установи), а m_2 їх кількість; 3) $\mathbf{E}$ – множина подій (порушень), які стали обставиною для оцінювання наслідків (шкоди), набуде вигляду [2]: $\mathbf{E} = \{\bigcup_{i=1}^{m_3} E_i\} = \{E_1, ..., E_{m_3}\}$, де $E_i \subseteq \mathbf{E}$ $(i = \overline{1, m_3})$ – i-та подія, а m_3 їх кількість $(m_3 = 2)$; 4) $\mathbf{A}$ – множина атак (подія-загроза), що призвела до появи $\boldsymbol{E}$, визначимо як [2]: $\mathbf{A} = \{\bigcup_{i=1}^{m_4} A_i\} = \{A_1, ..., A_{m_4}\}$, де $A_i \subseteq \mathbf{A}$ $(i = \overline{1, m_4})$ – i-та атака, а m_4 їх кількість; 5) $\mathbf{D}$ – множина відомостей, що становлять ДТ у вигляді номера статті ЗВДТ та їх ступінь секретності (СС) щодо яких відбулася подія $\mathbf{E}$, сформуємо як [2]:

$$\mathbf{D} = \{\bigcup_{i=1}^{m_5} \mathbf{D}_i\} = \{\bigcup_{i=1}^{m_5} \{\bigcup_{j=1}^{m_{5i}} \{\bigcup_{k=1}^{m_{5ij}} D_{ijk}\}\}\} = \{D_{1.1.1}, D_{1.1.2}, ..., D_{1.1.m_{51}}\}, \{D_{1.2.1}, D_{1.2.2}, ..., D_{1.2.m_{52}}\}, ...$$
$$\{D_{m_5.1.1}, D_{m_5.1.2}, ..., D_{m_5.m_{5m_{51}}.m_{5m_{5j}}}\}, (i = \overline{1, m_5},\ j = \overline{1, m_{5i}}, k = \overline{1, m_{5ij}});$$

6) $\mathbf{DS}$ – множина СС відомостей $\boldsymbol{D}$, набуде наступного виду [2]: $\mathbf{DS} = \{\bigcup_{i=1}^{m_6} DS_i\} = \{DS_1, ..., DS_{m_6}\}$, де $DS_i \subseteq \mathbf{DS}$ $(i = \overline{1, m_6})$ – i-та СС відомостей $\boldsymbol{D}$, а m_6 їх кількість $(m_6 = 3)$; 7) $\mathbf{T}$ – множина завдань з охорони ДТ (ОДТ) як комплекс k заходів (способів) з нейтралізації визначеного переліку можливих атак $\mathbf{A}$, визначається виразом [2]: $\mathbf{T} = \{\bigcup_{i=1}^{m_7} T_i\} = \{T_1, ..., T_{m_7}\}$, де $T_i \subseteq \mathbf{T}$ $(i = \overline{1, m_7})$ – i-те завдання, а m_7 їх кількість; 8) $\mathbf{CS}$ – множина значень коефіцієнту захищеності інформації в СРСД, відображається як [2]: $\mathbf{CS} = \{\bigcup_{i=1}^{m_8} CS_i\} = \{CS_1, ..., CS_{m_8}\}$, де $CS_i \subseteq \mathbf{CS}$ $(i = \overline{1, m_8})$ – i-те значення коефіцієнту захищеності інформації, а m_8 їх кількість $(m_8 = m_2)$; 9) $\mathbf{SW}$ – множина значень питомої ваги об'єкта відомостей $\mathbf{D}$, набуде вигляду [2]: $\mathbf{SW} = \{\bigcup_{i=1}^{m_9} SW_i\} = \{SW_1, ..., SW_{m_9}\}$, де $SW_i \subseteq \mathbf{SW}$ $(i = \overline{1, m_9})$ – i-те значення питомої ваги об'єкта відомостей $\boldsymbol{D}$, а m_9 їх кількість; 10) $\mathbf{L}$ – множина показників рівня зниження ефективності складової частини об'єкта (СЧО) відомостей $\boldsymbol{D}$, представимо виразом [2]: $\mathbf{L} = \{\bigcup_{i=1}^{m_{10}} L_i\} = \{L_1, ..., L_{m_{10}}\}$, де $L_i \subseteq \mathbf{L}$ $(i = \overline{1, m_{10}})$ – i-те значення рівня зниження ефективності СЧО відомостей $\boldsymbol{D}$, а m_{10} їх кількість; 11) $\mathbf{P}$ – множина значень відносної вартості СЧО відомостей $\boldsymbol{D}$, визначається як [2]: $\mathbf{P} = \{\bigcup_{i=1}^{m_{11}} P_i\} = \{P_1, ..., P_{m_{11}}\}$, де $P_i \subseteq \mathbf{P}$ $(i = \overline{1, m_{11}})$ – i-та відносна вартість СЧО, а m_{11} їх кількість; 12) $\mathbf{CA}$ – множина значень коефіцієнту морального старіння відомостей $\boldsymbol{D}$, набуде виду [2]: $\mathbf{CA} = \{\bigcup_{i=1}^{m_{12}} CA_i\} = \{CA_1, ..., CA_{m_{12}}\}$, де $CA_i \subseteq \mathbf{CA}$ $(i = \overline{1, m_{12}})$ – i-те значення коефіцієнту морального старіння відомостей $\boldsymbol{D}$, а m_{12} їх кількість $(m_{12} = m_5)$; 13) $\mathbf{TD}$ – множина показників сукупної шкоди, визначається виразом [2]: $\mathbf{TD} = \{\bigcup_{i=1}^{m_{13}} TD_i\} = \{TD_1, ..., TD_{m_{13}}\}$, де

$TD_i \subseteq \mathbf{TD}\ (i=\overline{1,m_{13}})$ – i-тий показник сукупної шкоди, а m_{13} їх кількість; 14) **LCT** – множина ідентифікаторів рівня класифікації терористичних загроз, має вигляд [3]: $\mathbf{LCT} = \{\bigcup_{m_{14}} LCT_i\} = \{LCT_1,...,LCT_{m_{14}}\}$, де $LCT_i \subseteq \mathbf{LCT}\ (i=\overline{1,m_{14}})$ – i-тий ідентифікатор рівня терористичної загрози, а m_{14} їх кількість ($m_{14}=4$).

У даному дослідженні запропоновано кортежну модель представлення базових параметрів оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави.

Література

1. 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 21-24 лютого 2018 р. – К.: Вид-во Європейський університет, 2018. – С.81-86.

2. Корченко О., Архипов О., Дрейс Ю. "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.

3. Корченко О., Дрейс Ю. "Додаткові критерії оцінювання шкоди, нанесеної розголошенням державної таємниці або втрати матеріальних носіїв секретної інформації за рівнем класифікації терористичних загроз", Актуальні проблеми забезпечення кібербезпеки та захисту інформації: тези доповідей учасників II Міжнародної науково-практичної конференції, 24-27 лютого 2016 р. – К: Вид-во Європейський університет, 2016. – С. 90-91.

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

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

УДК 342.1:355/359

Лебедєв О.Р.
кандидат юридичних наук, доцент
Національна академія СБ України

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ У ВІЙСЬКОВИХ УМОВАХ У КОНТЕКСТІ БОРОТЬБИ З ІНІЦІАТИВНИМ ШПИГУНСТВОМ

Процес становлення та розвитку України як незалежної держави з моменту проголошення суверенітету проходить в умовах складних геопо-