УДК 351.861

ОСОБЛИВОСТІ ОЦІНКИ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ У ПРОЦЕСІ ФУНКЦІОНУВАННЯ ЄДИНОЇ ДЕРЖАВНОЇ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ

В.В. Тютюник[1], док. тех. наук, професор, О.О. Тютюник[2], канд. техн. наук, доцент,
В.І. Заболотний[3], канд. техн. наук, доцент

[1] Національний університет цивільного захисту України
[2] Харківський національний економічний університет імені Семена Кузнеця
[3] Харківський національний університет радіоелектроніки

В Україні для забезпечення реалізації державної політики у сфері цивільного захисту функціонує Єдина державна система цивільного захисту (ЄДСЦЗ), яка складається з функціональних і територіальних підсистем та повинна забезпечувати необхідний рівень безпеки життєдіяльності в умовах надзвичайних ситуацій різної природи [1–3]. У процесі функціонування ЄДСЦЗ являє собою систему з рознесеними у просторі та часі складовими, які пов'язані між собою великими потоками різного роді інформації [4–7]. Показник ризику виникнення загроз для інформації, що циркулює у процесі функціонування ЄДСЦЗ, можливо представити як [8]:

$$R_{ЄДСЦЗ}^{Інформац} = \sum_{i=1}^{3} R_{ЄДСЦЗ\ i}^{Інформац}, \quad (1)$$

де $R_{ЄДСЦЗ\ 1}^{Інформац}$ – показник ризику для інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується розголошенням інформації; $R_{ЄДСЦЗ\ 2}^{Інформац}$ – показник ризику для інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується витоком інформації; $R_{ЄДСЦЗ\ 3}^{Інформац}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ.

Показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, включає наступні складові:

$$R_{ЄДСЦЗ\ 3}^{Інформац} = \sum_{k=1}^{3} R_{ЄДСЦЗ\ 3.k}^{Інформац}, \quad (2)$$

де $R_{ЄДСЦЗ\ 3.1}^{Інформац}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується втратою інформації; $R_{ЄДСЦЗ\ 3.2}^{Інформац}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується зміною інформації; $R_{ЄДСЦЗ\ 3.3}^{Інформац}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації.

Найбільш небезпечним з позицій інформаційної безпеки в даний час вважається несанкціонований доступ до комп'ютерної інформації. Показник ризику для комп'ютерної

інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації, включає наступні складові:

$$R_{ЄДСЦЗ\ з.з}^{Інформац.} = \sum_{g=1}^{9} R_{ЄДСЦЗ\ з.з.g}^{Інформац.}, \qquad (3)$$

де $R_{ЄДСЦЗ\ з.з.1}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом перегляду інформації (на екранах комп'ютерів, на друкуючих пристроях тощо); $R_{ЄДСЦЗ\ з.з.2}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом копіювання програм і даних (копіювання з інформаційних носіїв і жорстких дисків при слабкому захисті комп'ютерів, при поганій організації зберігання копій і архівів, при читанні даних по лініям зв'язку в мережах, при отриманні інформації за рахунок встановлення спеціальних закладок тощо); $R_{ЄДСЦЗ\ з.з.3}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни потоку повідомлень (в тому числі застосування закладок, що змінюють передану інформацію, при тому, що на екрані вона залишається без змін); $R_{ЄДСЦЗ\ з.з.4}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни конфігурації комп'ютерних засобів (зміна прокладки кабелів, зміна комплектації комп'ютерів і периферійних пристроїв під час технічного обслуговування, завантаження сторонньої операційної системи для доступу до інформації, встановлення додаткового порту для зовнішнього пристрою тощо); $R_{ЄДСЦЗ\ з.з.5}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни розташування комп'ютерних засобів та/або режиму обслуговування та умов експлуатації. Це – установка додаткових пристроїв поблизу комп'ютерів (систем пожежної та охоронної сигналізації, телефонних мереж, систем електроживлення тощо), зміни розташування комп'ютерів для поліпшення доступу до інформації (візуального спостереження); $R_{ЄДСЦЗ\ з.з.6}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом несанкціонованої модифікації контрольних процедур (наприклад, при перевірці аутентичності електронного підпису, якщо він виконується програмними засобами); $R_{ЄДСЦЗ\ з.з.7}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом підробки та/або додавання об'єктів, які не є легальними, але володіють основними властивостями легальних об'єктів (наприклад, додавання підроблених записів в файл). Особливо це небезпечно при використанні систем автоматизованого обліку різних об'єктів; $R_{ЄДСЦЗ\ з.з.8}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом додавання фальшивих процесів та/або підміна справжніх процесів обробки даних фальшивими. Це відноситься як до роботи операційних систем, так і особливо до роботи пакетів прикладних

програм; $R_{ЄДСЦЗ\ 3.3.9}^{Інформац\ \cdot}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ЄДСЦЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом фізичного руйнування апаратних засобів або переривання функціонування комп'ютерних засобів різними способами з метою часткового або повного знищення інформації, що зберігається.

При одночасному впливі на інформацію, що циркулює у процесі функціонування ЄДСЦЗ, декількох процесів небезпеки, необхідно враховувати можливість прояву синергетичного ефекту [9, 10]. У цьому випадку імовірність перевищення нормативного показника для двох спільних аспектів небезпеки для інформації, що обертається у процесі функціонування ЄДСЦЗ можна розрахувати як:

$$P_{ЄДСЦЗ\ i.j}^{Інформац\ \cdot} = P_{ЄДСЦЗ\ i.1}^{Інформац\ \cdot} + P_{ЄДСЦЗ\ i.2}^{Інформац\ \cdot} - P_{ЄДСЦЗ\ i.1}^{Інформац\ \cdot} \cdot P_{ЄДСЦЗ\ i.2}^{Інформац\ \cdot}. \quad (4)$$

Таким чином, в роботі представлено результати розповсюдження ризико-орієнтованого підходу для оцінки виникнення загроз для інформації, що циркулює у процесі функціонування ЄДСЦЗ, як системи з рознесеними у просторі та часі складовими, які пов'язані між собою великими потоками різного роді інформації. Представлені результати є однією з складових комплексного підходу щодо розвитку наукових основ формування системи національної безпеки держави.

ЛІТЕРАТУРА

1. Кодекс цивільного захисту України від 2 жовтня 2012 року № 5403-VI // Голос України. – 2012.– листопад (№ 220(5470)). – С. 4 – 20.
2. Постанова Кабінету Міністрів України від 9 січня 2014 року № 11 «Про затвердження Положення про Єдину державну систему цивільного захисту» [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/11-2014-%D0%BF
3. Розпорядження Кабінету Міністрів України від 25 січня 2017 року № 61-р. «Про схвалення Стратегії реформування системи Державної служби України з надзвичайних ситуацій» [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/61-2017-%D1%80
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016
6. Постанова кабінету міністрів України від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
7. Наказ ДСНС від 01 жовтня 2020 року № 533 «Про затвердження Положення з організації заходів забезпечення кібербезпеки ДСНС».
8. Рубан І.В., Тютюник В.В., Заболотний В.І., Тютюник О.О. Особливості розповсюдження ризико-орієнтованого підходу до оцінки вразливості об'єктів кіберзахисту. *Науковий журнал "Безпека інформації"*. Київ: Національний авіаційний університет, 2020. Т.26. №3. С. 145–155.
9. Малинецкий Г.Г. Математические основы синергетики: Хаос, структуры, вычислительный эксперимент. Москва: Книжный дом «ЛИБРОКОМ», 2012, 312 с.
10. Тютюник В.В., Писклакова О.О. Теорія систем та системний аналіз. Харків: Національний університет цивільного захисту України, 2020, 104 с.