МОДЕЛЮВАННЯ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Охрімчук В. В., , Самчишин О. В.
Житомирський військовий інститут імені. С. П. Корольова, м. Житомир

Інформаційна безпека держави нині й у найближчому майбутньому залишатиметься одним із головних безпекових індикаторів стійкості України до нових викликів та загроз у кіберпросторі. Особливо гостро в умовах воєнної агресії проти України стоять питання забезпечення кібербезпеки об'єктів критичної інфраструктури.

Вивчення теорії та практики забезпечення кібербезпеки показало, що для виведення з ладу об'єктів критичної інформаційної інфраструктури держави, зловмисником або протиборчою стороною здійснюються потенційно небезпечні високотехнологічні кібератаки (КбА).

Враховуючи важливість об'єктів критичної інфраструктури для їх захисту від КбА, як правило, використовується не одна, а декілька систем інформаційної безпеки (СІБ), кожна з яких працює на певному рівні та направлена для виявлення та нейтралізації певних видів КбА, використовуючи для цього свою базу знань про раніше виявлені КбА, на основі якої будуються еталонні моделі (сигнатури) за якими відбувається виявлення.

В основу функціонування таких СІБ покладені різні технології та механізми протидії. З аналізу методів, покладених в основу їх функціонування встановлено, що в більшості вони ґрунтуються на сигнатурних підходах до виявлення КбА, які характеризуються наявністю "ефекту запізнення" з вироблення потрібної сигнатури. Наявність даного ефекту суттєво ускладнює, а в деяких випадках унеможливлює виявлення потенційно небезпечних КбА.

Тому для побудови моделі (сигнатури) потенційно небезпечних КбА пропонується провести синтез СІБ, які використовуються для кіберзахисту об'єкта критичної інформаційної інфраструктури, та їх баз знань з метою розширення ознакового простору параметрів за якою СІБ приймає рішення про здійснення на об'єкт критичної інформаційної інфраструктури КбА конкретного типу. Такий підхід дає змогу розробити модель, яка зможе всебічно описати ознаки потенційно небезпечної КбА, які необхідні для побудови відповідних сигнатур. Крім того використання запропонованого підходу на практиці дає змогу скористатися принципом комплексування баз знань СІБ про КбА, взявши з кожної з них їх переваги та взаємокомпенсувавши існуючі недоліки.

Отже, запропонований підхід до побудови моделей потенційно небезпечних КбА на об'єкти критичної інфраструктури ґрунтується на одночасному визначенні базових характеристик і параметрів (ознак) таких атак на основі всебічного аналізу баз знань про виявлені раніше КбА та дозволяє нівелювати вплив "ефекту запізнення" в ході створення сигнатур. Такий підхід дає змогу на 15% підвищити ефективність виявлення потенційно небезпечних КбА на об'єкти критичної інфраструктури порівняно з найкращими із діючих зразків СІБ, які використовуються на практиці, зокрема, NOD32 Eset.