УДК 004.05

О.О. ЛЕТИЧЕВСЬКИЙ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *oleksandr.letychevskyi@litsoft.com.ua.*

НЕЙРОСИМВОЛЬНІ ДВІЙНИКИ ПРОГРАМНИХ СИСТЕМ ТА ЇХНЄ ВИКОРИСТАННЯ У РОЗВ'ЯЗАННІ ЗАДАЧ КІБЕРБЕЗПЕКИ

Анотація. Розглянуто використання двійників програмних систем, які є комбінацією алгебраїчної моделі та нейронної мережі. Досліджено застосування цієї технології в системах виявлення вторгнень та на етапі оцінювання надійності кіберзахисту програмних систем. Зауважено, що пропонований підхід може забезпечити значне підвищення точності виявлення кібератак у реальному часі та протидію змагальним атакам, а також дасть змогу уникнути хибних виявлень, що є проблемою у виявленні атак з невідомою семантикою. Проаналізовано використання нейросимвольного двійника на етапі підготовки системи до функціонування, а саме процедуру виявлення вразливостей системи. Представлено архітектуру системи виявлення вторгнень на основі нейросимвольного двійника з можливістю моніторінгу вхідного комунікаційного протоколу та функцію відновлення програмного середовища. Наведено приклади використання технології у блокчейн-середовищі та в захисті апаратного забезпечення.

Ключові слова: цифровий двійник, кібербезпека, алгебраїчне моделювання, нейронна мережа глибокого навчання, змагальні атаки, пошук уразливостей, система виявлення вторгнень.

ВСТУП

Проблема кібербезпеки завжди була в центрі уваги наукової спільноти, оскільки від надійного захисту та протидії кібератаці на об'єкти критичної інфраструктури залежить спроможність державних структур та виробництва до нормального функціонування. Можливість протидіяти вторгненням в інформаційні ресурси зазвичай забезпечували за допомогою низки різних технологій. Якщо перші програми захисту містили шаблони атак або вірусів, то вже сьогодні методи штучного інтелекту набули широкого застосування у класифікації вторгнень, зокрема злоякісного інтернет-трафіку. Через те, що в умовах сучасної кібервійни засоби вторгнень постійно вдосконалюються, для захисту застосовують більш складні гібриди технологій. Їхні переваги створюють синергію, яка суттєво впливає на ефективність захисту.

У статті розглянуто комбінацію трьох технологій, а саме нейронних мереж, алгебраїчного або символьного підходу та технології цифрових двійників. Також запропоновано архітектуру системи виявлення вторгнень, яка використовує ці три складові для підвищення ефективності захисту, протидії та стійкості.

ТЕХНОЛОГІЯ ЦИФРОВИХ ДВІЙНИКІВ

Поняття цифрового двійника (digital twin) або цифрового близнюка системи чи об'єкта нині застосовують у багатьох галузях індустрії. Ідею цифрового двійника вперше визначив Майкл Грівз ще у 2002 р., тоді як перше визначення цього терміна в літературі було надано в [11] у 2016 р. Цифровий двійник є віртуальною копією системи, яка сприймає дані із зовнішнього середовища. Його досліджують на властивості або моделюють під час функціонування оригіналу системи чи її підготовки. Цифрові двійники використовують в охороні здоров'я, автомобільній промисловості, морському судноплавстві, аерокосмічній галузі, управлінні містом та в багатьох інших галузях. Уперше цифровий двійник застосували під час місії Apollo 13. Під час високоточної симуляції диспетчери NASA змогли оперативно адаптувати та змінювати сценарії, що відповідали реальним умовам вибуху кисневого бака на борту й