

УДК 004.94:681.5

Шаптала С.В.¹, Воскобойник В.О.²

¹ старш. викл. НУ «Запорізька політехніка»

² канд. техн. наук, доц. НУ «Запорізька політехніка»

ЦИФРОВІ ДВІЙНИКИ У ПРОАКТИВНОМУ ВИЯВЛЕННІ ТА РЕАГУВАННІ НА КІБЕРЗАГРОЗИ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВА

У сучасному світі телекомунікаційні системи підприємств стають все більш уразливими до кіберзагроз через зростання обсягу оброблюваних даних та складність інфраструктури. Забезпечення безпеки цих систем є критично важливим для збереження конфіденційної інформації, підтримки безперебійної роботи бізнес-процесів та захисту репутації організацій. Використання цифрових двійників (Digital Twins) стає перспективним напрямком у сфері кібербезпеки, оскільки вони надають можливість створення віртуальних реплік фізичних систем для прогнозного аналізу та моделювання різноманітних сценаріїв атак. Цифрові двійники не лише імітують фізичні компоненти, але й інтегрують дані з різних сенсорів, що дозволяє здійснювати детальний моніторинг та аналіз поведінки систем у реальному часі.

Актуальність цього дослідження полягає в необхідності розробки ефективних моделей та методів забезпечення кібербезпеки в телекомунікаційних системах підприємств. Зростаюча кількість та складність кібератак вимагають нових підходів до захисту інформаційних систем, а цифрові двійники пропонують інноваційні рішення, які можуть значно підвищити рівень захисту та знизити ризики. Метою дослідження є визначення ефективності використання цифрових двійників у проактивному виявленні та реагуванні на кіберзагрози в телекомунікаційних системах підприємств. Це включає теоретичний аналіз існуючих моделей, розробку концептуальної моделі цифрового двійника для кібербезпеки та проведення порівняльного аналізу з традиційними методами захисту.

Цифрові двійники мають потенціал значно покращити процеси виявлення та реагування на кіберзагрози через моделювання різних сценаріїв атак та автоматизацію відповідних заходів захисту. Вони дозволяють створювати специфічні віртуальні репліки інфраструктури підприємства, що забезпечує адаптовану прогнозну аналітику та персоналізовані заходи захисту. Це сприяє проактивному підходу до кібербезпеки, де компанії можуть не лише реагувати на вже виниклі загрози, але й передбачати можливі атаки та відповідно готуватися до них. Автоматизація процесів виявлення та усунення слабких місць у системах підвищує ефективність персоналу та зміцнює безпеку на всіх рівнях, дозволяючи швидко ідентифікувати та усувати потенційні загрози.



Рисунок 1 - Цифрові двійники у кібербезпеці

Вибір цифрових двійників обґрунтовується їх здатністю забезпечувати точний та детальний аналіз поведінки систем у різних умовах. Це дозволяє проводити експерименти з кіберзахистом на всіх рівнях системи, готуючи сценарії "що-якщо" та забезпечуючи охоплення всіх можливих випадків. Крім того, цифрові двійники сприяють підвищенню кіберстійкості підприємств, забезпечуючи можливість швидкої адаптації до змінних умов та нових загроз. Це особливо важливо в умовах динамічних та швидко еволюціонуючих кіберзагроз, де можливість оперативного реагування на нові ризики може визначати успіх у забезпеченні безпеки інформаційних систем.

Для дослідження було проведено аналіз існуючих літературних джерел та симуляційні тести у віртуальному середовищі. Дослідження ґрунтується на методології теоретичного аналізу, розробці концептуальної моделі цифрового двійника для кібербезпеки та проведенні порівняльного аналізу з традиційними методами захисту. Це дозволяє всебічно оцінити ефективність запропонованих моделей та визначити їхні переваги у порівнянні з існуючими підходами.

Таким чином, впровадження цифрових двійників у телекомунікаційних системах підприємств представляє собою інноваційний підхід до забезпечення кібербезпеки. Це дозволяє не лише ефективно виявляти та реагувати на загрози, але й значно підвищувати загальну стійкість та безпеку інформаційних систем підприємств. Використання цифрових двійників сприяє підвищенню ефективності заходів захисту та скороченню часу реагування, роблячи їх важливим інструментом для сучасних підприємств з високими вимогами до свого захисту.