УДК 004.85:004.056

РОЛЬ НАВЧАННЯ З ПІДКРІПЛЕННЯМ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ВІД ЕЛЕКТРОННОГО ШАХРАЙСТВА

Вельма І.Ю.,
Науковий керівник – д. т. н., проф. Мартинчук О. О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: ihor.velma@nure.ua

In today's digital age, where technology permeates every aspect of our lives, cybersecurity has emerged as a paramount concern. With the exponential growth of online transactions, communication, and data storage, the threat of electronic fraud, commonly known as cybercrime, has become more pervasive and sophisticated than ever before. In response to this evolving landscape, organizations worldwide are continuously striving to fortify their defense mechanisms against cyber threats.

Навчання з підкріпленням (reinforcement learning) є методом машинного навчання, який базується на використанні системи нагород та покарань для навчання агента. У контексті кібербезпеки, цей підхід може бути дуже корисним, оскільки дозволяє створювати адаптивні та ефективні системи захисту, які вчаться на власних помилках та уникають їх у майбутньому. У сфері кібербезпеки, навчання з підкріпленням може бути використане для навчання систем виявлення загроз або іншого програмного забезпечення взаємодіяти з ними. Наприклад, агент може отримувати позитивну нагороду за виявлення підозрілого трафіку та відповідне реагування на нього, або негативну нагороду за пропуск потенційно шкідливих дій. Один з головних переваг навчання з підкріпленням в кібербезпеці є можливість адаптувати систему захисту до змінюючихся умов і загроз. Система може навчитися реагувати на нові види атак або змінювати свою стратегію захисту відповідно до нових обставин. Це дозволяє забезпечити більш ефективний захист від кібератак та зменшити ймовірність успішних атак. Крім того, навчання з підкріпленням допомагає зрозуміти, які дії є найбільш ефективними в конкретних ситуаціях. Аналізуючи реакції системи на різні види загроз, можна виявити слабкі місця та вдосконалити стратегії захисту [1].

Проведення симуляцій та тренувань дозволяє нейромережі отримати практичний досвід виявлення та реагування на потенційні загрози електронного шахрайства в контрольованих обставинах. Під час симуляцій відтворюються ситуації, що можуть виникнути в реальному житті, проте в контрольованому середовищі. Наприклад, можна використовувати програмне забезпечення для моделювання атак на комп'ютерні мережі або імітацію спам-атак на електронну пошту. Спеціалістам з кібербезпеки

дається можливість взаємодіяти з цими сценаріями, аналізувати їх і реагувати на них, не ризикуючи безпекою реальних систем. Тренування включає в себе систематичну практику та навчання нейромережі засобам виявлення та протидії електронному шахрайству. Це може бути проведено у формі рольових ігор, симуляційних вправ або інтерактивних тренажерів. Під час тренувань нейромережа отримує можливість працювати з реальними інцидентами, навчаючись розпізнавати загрози та вживати необхідні заходи для їх подолання.

Навчання нейромережі на реальних прикладах є дієвим методом для покращення розуміння конкретних загроз електронного шахрайства та їх реальних наслідків. Використання реальних прикладів електронного шахрайства дозволяє персоналу отримати практичний досвід у роботі з нейромережами. Це допомагає їм краще зрозуміти як нейромережі можуть застосовуватися для виявлення та протидії кіберзагрозам. Робота з реальними випадками електронного шахрайства дозволяє персоналу аналізувати реальні наслідки кібератак. Це допомагає їм краще зрозуміти масштаб та серйозність потенційних загроз та прийняти відповідні заходи захисту. Робота з реальними прикладами надає персоналу можливість навчитися практичним навичкам розробки та налаштування нейромереж для виявлення та запобігання кіберзагрозам.

Оновлення навчальних програм у сфері кібербезпеки є критично важливим процесом для забезпечення ефективної підготовки персоналу до боротьби зі сучасними кіберзагрозами. Швидкі технологічні зміни в кіберпросторі вимагають постійного оновлення навчальних програм, щоб вони відповідали сучасним методам та інструментам захисту. Наприклад, із зростанням використання штучного інтелекту та машинного навчання в кібератаках, навчальні програми повинні включати в себе вивчення цих технологій для розпізнавання та протидії їхнім використанням в атаках. Нові методи атак вимагають розробки та вдосконалення стратегій оборони. Оновлені навчальні програми повинні враховувати ці стратегії та навички для ефективного запобігання та виявлення кіберзагроз.

Навчання з підкріпленням може стати потужним інструментом в підвищенні ефективності систем захисту від електронного шахрайства. Використання випереджаючих стратегій та урахування практичних аспектів навчання може допомогти створити адаптивні та надійні системи захисту, які здатні ефективно протистояти сучасним кіберзагрозам.

Список використаних джерел:

1. Навчання з підкріпленням у машинному навчанні. URL: https://evergreens.com.ua/ua/articles/reinforcement-learning.html (дата звернення: 28.02.2024)