Овсянко Дмитро Сергійович, студент 2 курсу факультету природничої та фізико-математичної освіти, Глухівський національний педагогічний університет імені Олександра Довженка, Україна, ORCID ID: 0009-0003-1830-8441

Ovsianko Dmytro Serhiyovych, 2nd year student, Faculty of Natural Science and Physics-Mathematics Education Oleksandr Dovzhenko, Hlukhiv National Pedagogical University, Ukraine, ORCID ID: 0009-0003-1830-8441

ВИКОРИСТАННЯ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНОЇ МЕРЕЖЕВОЇ АКТИВНОСТІ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

USING DEEP NEURAL NETWORKS TO DETECT ANOMALOUS NETWORK ACTIVITY IN REAL-TIME

Анотація

У статті досліджено можливості застосування глибоких нейронних мереж для виявлення аномальної мережевої активності в режимі реального часу. Проведено аналіз сучасних підходів до забезпечення кібербезпеки комп'ютерних мереж, розглянуто особливості функціонування систем виявлення вторгнень та визначено основні переваги використання методів глибокого навчання для аналізу мережевого трафіку. Особливу увагу приділено архітектурам CNN, RNN, LSTM та Autoencoder, які широко застосовуються для класифікації мережевих подій і виявлення аномалій. Визначено перспективи використання глибоких нейронних мереж у сучасних системах кіберзахисту.

Ключові слова: кібербезпека, штучний інтелект, глибоке навчання, нейронні мережі, мережевий трафік, аномалії, системи виявлення вторгнень

Abstract

The article explores the possibilities of using deep neural networks to detect anomalous network activity in real time. An analysis of modern approaches to ensuring cybersecurity of computer networks is conducted, the features of the functioning of intrusion detection systems are considered, and the main advantages of using deep learning methods for analyzing network traffic are identified. Particular attention is paid to the CNN, RNN, LSTM, and Autoencoder architectures, which are widely used for classifying network events and detecting anomalies. The prospects for using deep neural networks in modern cyber defense systems are identified.

Keywords: cybersecurity, artificial intelligence, deep learning, neural networks, network traffic, anomalies, intrusion detection systems

Стрімкий розвиток інформаційних технологій супроводжується збільшенням кількості кіберзагроз, спрямованих на комп'ютерні мережі та інформаційні системи. Традиційні методи виявлення атак, які базуються на сигнатурному аналізі, часто виявляються недостатньо ефективними для протидії новим та модифікованим типам загроз. У зв'язку з цим особливого значення набуває використання технологій штучного інтелекту, зокрема глибоких нейронних мереж, здатних автоматично аналізувати великі обсяги мережевого трафіку та виявляти приховані закономірності поведінки зловмисників.

Проблема виявлення мережевих атак за допомогою методів машинного навчання активно досліджується протягом останнього десятиліття. У сучасних наукових роботах значна увага приділяється

застосуванню алгоритмів класифікації, ансамблевих методів та глибоких нейронних мереж для підвищення точності систем виявлення вторгнень. Результати досліджень свідчать про те, що моделі глибокого навчання забезпечують вищий рівень точності порівняно з традиційними підходами завдяки здатності самостійно виділяти інформативні ознаки з великих наборів даних [1, 2].

Метою дослідження є аналіз ефективності використання глибоких нейронних мереж для виявлення аномальної мережевої активності в режимі реального часу та визначення перспектив їх впровадження у сучасні системи кібербезпеки.

Актуальність дослідження обумовлена також стрімкою цифровізацією суспільства, розвитком хмарних технологій, Інтернету речей (IoT), мобільних сервісів та розподілених інформаційних систем. Зі збільшенням кількості підключених пристроїв суттєво зростає площа потенційних атак, що створює додаткові виклики для забезпечення інформаційної безпеки. За даними міжнародних аналітичних центрів, щороку спостерігається зростання кількості складних цілеспрямованих атак, програм-вимагачів, ботнетів та інших видів кіберзагроз, здатних завдавати значних фінансових та репутаційних збитків організаціям [8, 9, 10].

Традиційні системи виявлення вторгнень (Intrusion Detection Systems, IDS) переважно використовують сигнатурний підхід, який базується на пошуку відомих шаблонів атак. Незважаючи на високу ефективність під час виявлення вже відомих загроз, такі системи мають суттєві обмеження при протидії новим або модифікованим атакам. Крім того, сучасний мережевий трафік характеризується високою інтенсивністю та різноманітністю, що ускладнює його аналіз за допомогою традиційних методів [6].

У зв'язку з цим все більшої популярності набувають інтелектуальні методи аналізу даних, засновані на алгоритмах машинного та глибокого

навчання. Глибокі нейронні мережі дозволяють автоматично виявляти складні взаємозв'язки між характеристиками мережевого трафіку, виконувати класифікацію подій та прогнозувати можливі загрози без необхідності ручного створення правил або сигнатур. Завдяки багаторівневій структурі такі моделі здатні формувати високорівневі ознаки з необроблених даних, що значно підвищує ефективність виявлення аномалій.

Особливий інтерес для дослідників становить використання архітектур глибокого навчання під час аналізу мережевого трафіку в режимі реального часу. У таких системах важливими є не лише точність класифікації, але й швидкість прийняття рішень, оскільки навіть незначна затримка може призвести до успішної реалізації атаки та компрометації інформаційних ресурсів. Саме тому сучасні дослідження спрямовані на створення моделей, які здатні забезпечувати високу продуктивність при обробці великих потоків даних та оперативно реагувати на виникнення підозрілої активності.

Слід зазначити, що застосування глибоких нейронних мереж у сфері кібербезпеки відкриває нові можливості для побудови адаптивних систем захисту. Такі системи можуть постійно вдосконалюватися в процесі експлуатації, накопичувати нові знання про загрози та автоматично адаптуватися до змін у мережевому середовищі. Це особливо актуально в умовах швидкої еволюції кіберзагроз та появи нових методів атак, які часто залишаються непоміченими для традиційних засобів захисту.

Таким чином, дослідження можливостей використання глибоких нейронних мереж для виявлення аномальної мережевої активності є важливим науковим і практичним завданням, вирішення якого сприятиме підвищенню ефективності сучасних систем кібербезпеки та забезпеченню надійного захисту інформаційних ресурсів від кіберзагроз.

Аномальна мережева активність як об'єкт дослідження

Аномальною мережевою активністю вважаються будь-які відхилення від нормального функціонування мережі, які можуть свідчити про наявність кіберзагроз. До таких загроз належать DDoS-атаки, мережеве сканування, ботнет-активність, спроби несанкціонованого доступу та поширення шкідливого програмного забезпечення.

Своєчасне виявлення подібних аномалій є одним із ключових завдань систем кіберзахисту, оскільки дозволяє мінімізувати потенційні збитки та запобігти компрометації інформаційних ресурсів. У сучасних комп'ютерних мережах обсяги передаваних даних постійно зростають, що значно ускладнює процес моніторингу та аналізу мережевого трафіку. Крім того, кіберзлочинці постійно вдосконалюють методи атак, використовуючи нові інструменти та технології для обходу традиційних систем захисту.

Особливу небезпеку становлять атаки, які маскуються під звичайну активність користувачів та не містять характерних ознак відомих загроз. Такі атаки можуть тривалий час залишатися непоміченими, поступово збираючи конфіденційну інформацію або створюючи умови для подальшого проникнення до інформаційної системи. Саме тому сучасні системи кібербезпеки дедалі частіше орієнтуються не лише на виявлення відомих шаблонів атак, а й на аналіз поведінкових характеристик мережевого трафіку.

До найбільш поширених видів аномальної мережевої активності належать атаки типу DDoS (Distributed Denial of Service), метою яких є перевантаження мережевих ресурсів та порушення доступності сервісів. Такі атаки можуть здійснюватися одночасно з великої кількості заражених пристроїв, об'єднаних у ботнет-мережі. Не менш небезпечними є атаки сканування мережі, під час яких зловмисники збирають інформацію про відкриті порти, мережеві служби та потенційні вразливості системи.

Ще одним видом аномальної активності є спроби підбору облікових даних (Brute Force Attack), які полягають у багаторазовому надсиланні запитів на автентифікацію з різними комбінаціями логінів і паролів. Подібні дії можуть свідчити про спробу отримання несанкціонованого доступу до інформаційних ресурсів. Крім того, значну загрозу становить поширення шкідливого програмного забезпечення через мережеві канали зв’язку, що може призводити до втрати даних, порушення роботи інформаційних систем або викрадення конфіденційної інформації [7].

Для ефективного виявлення аномалій необхідно здійснювати безперервний моніторинг мережевого середовища та аналізувати широкий спектр параметрів мережевого трафіку. До таких параметрів належать кількість пакетів, швидкість передачі даних, тривалість з'єднань, характеристики протоколів, адреси джерела та призначення, а також поведінкові особливості користувачів і мережевих пристроїв. Аналіз цих показників дозволяє виявляти відхилення від нормальної роботи мережі та своєчасно реагувати на потенційні загрози.

У сучасних умовах особливого значення набуває використання методів машинного та глибокого навчання для автоматизованого виявлення аномальної активності. Такі методи дозволяють аналізувати великі обсяги мережевих даних у режимі реального часу та виявляти складні закономірності, які важко визначити за допомогою традиційних алгоритмів. Завдяки цьому забезпечується підвищення точності виявлення кіберзагроз та зменшення кількості хибнопозитивних спрацювань систем захисту.

Таким чином, аномальна мережева активність є важливим об'єктом дослідження у сфері кібербезпеки, а розробка ефективних методів її виявлення залишається одним із пріоритетних напрямів розвитку сучасних інформаційних технологій та систем захисту інформації.

Використання глибоких нейронних мереж для аналізу мережевого трафіку

Глибокі нейронні мережі являють собою багаторівневі математичні моделі, здатні виконувати автоматичне виділення ознак та класифікацію даних. Для аналізу мережевого трафіку найчастіше використовуються такі архітектури:

Convolutional Neural Networks (CNN). Дані моделі забезпечують ефективне виділення локальних закономірностей у великих масивах мережевих даних та демонструють високу швидкість обробки інформації [3].

Recurrent Neural Networks (RNN). Використовуються для аналізу послідовностей подій у мережевому трафіку та дозволяють враховувати часові залежності між мережевими пакетами [2].

Long Short-Term Memory (LSTM). Є вдосконаленою версією рекурентних мереж і забезпечує більш точне виявлення довгострокових залежностей у даних, що особливо важливо під час аналізу складних кібератак [4].

Autoencoder. Використовується для виявлення аномалій шляхом порівняння вхідних даних із реконструйованими моделлю даними. Значне відхилення свідчить про можливу аномальну активність [5].

Кожна з наведених архітектур має свої особливості та переваги залежно від типу даних і поставлених завдань. Вибір конкретної моделі визначається характером мережевого трафіку, вимогами до швидкості обробки інформації та необхідним рівнем точності виявлення загроз. У багатьох сучасних дослідженнях використовуються комбіновані підходи, які поєднують можливості кількох архітектур одночасно для досягнення максимальної ефективності.

Процес аналізу мережевого трафіку за допомогою глибоких нейронних мереж зазвичай складається з декількох етапів. На першому етапі

здійснюється збір мережевих даних із різних джерел, таких як маршрутизатори, комутатори, міжмережеві екрани та системи моніторингу мережі. Отримані дані проходять процедури попередньої обробки, які включають очищення від помилкових записів, нормалізацію параметрів та перетворення даних у формат, придатний для навчання нейронної мережі.

Наступним етапом є виділення характеристик мережевого трафіку. До таких характеристик можуть належати тривалість мережевого з'єднання, кількість переданих пакетів, обсяг переданих даних, частота звернень до певних ресурсів, використані протоколи зв'язку та інші параметри. У традиційних системах ці ознаки формуються експертами вручну, тоді як моделі глибокого навчання здатні автоматично визначати найбільш інформативні характеристики без участі людини.

Після завершення підготовки даних виконується навчання моделі на спеціалізованих наборах даних, що містять приклади як нормального мережевого трафіку, так і різних видів атак. У процесі навчання нейронна мережа поступово коригує власні параметри для мінімізації помилок класифікації та підвищення точності прогнозування. Після завершення навчання модель може використовуватися для аналізу нових даних у режимі реального часу.

Однією з головних переваг глибоких нейронних мереж є їх здатність виявляти раніше невідомі типи атак. На відміну від сигнатурних систем, які можуть розпізнавати лише відомі загрози, моделі глибокого навчання аналізують загальні закономірності поведінки мережевого трафіку та здатні виявляти суттєві відхилення від нормальної роботи мережі. Це особливо важливо в умовах постійної появи нових видів шкідливого програмного забезпечення та складних багатоетапних атак.

Крім того, глибокі нейронні мережі демонструють високу ефективність при роботі з великими обсягами даних. Сучасні корпоративні

мережі генерують мільйони мережевих пакетів щодня, що робить ручний аналіз практично неможливим. Використання технологій штучного інтелекту дозволяє автоматизувати процес моніторингу мережі та значно скоротити час реагування на потенційні загрози.

Важливою перевагою є також можливість роботи систем у режимі реального часу. Завдяки розвитку високопродуктивних графічних процесорів та спеціалізованих обчислювальних платформ сучасні нейронні мережі здатні аналізувати великі потоки мережевого трафіку практично без затримок. Це дозволяє своєчасно виявляти атаки та оперативно застосовувати механізми захисту для запобігання негативним наслідкам.

Останні дослідження демонструють, що точність сучасних моделей глибокого навчання при виявленні мережевих атак може перевищувати 95–99 %, залежно від типу використаних даних та архітектури нейронної мережі. Такі результати підтверджують перспективність використання технологій глибокого навчання як одного з ключових напрямів розвитку сучасних систем кібербезпеки [1, 3, 4, 5].

Переваги використання глибокого навчання

Використання глибоких нейронних мереж у системах виявлення вторгнень (IDS) та аналізу мережевого трафіку має низку суттєвих переваг порівняно з традиційними методами машинного навчання та сигнатурними підходами. Насамперед такі моделі забезпечують високу точність класифікації мережевого трафіку завдяки здатності аналізувати складні закономірності та взаємозв’язки між великою кількістю параметрів мережевих пакетів.

Однією з найважливіших переваг є можливість виявлення раніше невідомих атак. На відміну від класичних систем, які орієнтуються переважно на заздалегідь визначені сигнатури загроз, глибокі нейронні

мережі здатні визначати аномальну поведінку в мережі та виявляти нові типи атак, для яких ще не створено відповідних правил або шаблонів.

Важливою особливістю глибокого навчання є автоматичне виділення та формування ознак. Традиційні методи часто потребують участі експертів для ручного відбору характеристик мережевого трафіку, тоді як нейронні мережі самостійно знаходять найбільш інформативні ознаки під час процесу навчання. Це дозволяє значно спростити розробку системи та підвищити її ефективність.

Ще однією перевагою є здатність працювати з великими обсягами даних у режимі реального часу. Сучасні комп'ютерні мережі генерують величезну кількість інформації, яку необхідно аналізувати без затримок. Архітектури глибокого навчання можуть ефективно обробляти такі потоки даних, забезпечуючи своєчасне виявлення підозрілої активності.

Крім того, нейронні мережі характеризуються високою адаптивністю до нових кіберзагроз. Завдяки можливості повторного навчання та оновлення моделей система може враховувати нові типи атак і зміни в поведінці мережевого трафіку без необхідності повної перебудови механізмів захисту.

Таким чином, застосування глибокого навчання у сфері кібербезпеки дозволяє підвищити точність виявлення вторгнень, зменшити кількість хибних спрацьовувань, автоматизувати процес аналізу даних та забезпечити ефективний захист мережевої інфраструктури від сучасних кіберзагроз.

Проблеми та обмеження використання глибоких нейронних мереж

Незважаючи на високу ефективність глибоких нейронних мереж у задачах аналізу мережевого трафіку та виявлення кіберзагроз, їх практичне використання супроводжується низкою проблем і обмежень. Однією з головних труднощів є значна потреба в обчислювальних ресурсах. Навчання складних моделей глибокого навчання потребує використання потужних

графічних процесорів (GPU) або спеціалізованих обчислювальних платформ, що може суттєво збільшувати вартість впровадження та експлуатації таких систем.

Ще однією важливою проблемою є необхідність наявності великих обсягів якісних навчальних даних. Для досягнення високої точності нейронні мережі повинні навчатися на репрезентативних наборах мережевого трафіку, які містять як нормальну активність, так і різні типи атак. Формування таких вибірок є складним завданням через швидкий розвиток кіберзагроз та обмежену доступність актуальних даних.

Суттєвим недоліком глибокого навчання залишається складність інтерпретації результатів роботи моделей. Більшість сучасних нейронних мереж функціонують за принципом так званої «чорної скриньки», коли користувач або фахівець з кібербезпеки не може однозначно визначити, які саме фактори вплинули на прийняття рішення системою. Це ускладнює аналіз помилок, аудит безпеки та підвищення довіри до автоматизованих систем виявлення вторгнень.

Крім того, навіть високоточні моделі можуть генерувати хибнопозитивні та хибнонегативні спрацювання. У першому випадку легітимний мережевий трафік помилково визначається як загроза, що призводить до зайвих попереджень та перевантаження адміністраторів безпеки. У другому випадку реальна атака може залишитися невиявленою, що створює додаткові ризики для інформаційної інфраструктури.

Окремою проблемою є необхідність регулярного оновлення моделей. Характер мережевого трафіку та методи проведення кібератак постійно змінюються, тому моделі, навчені на застарілих даних, можуть втрачати свою ефективність. Це вимагає періодичного перенавчання систем та впровадження механізмів адаптації до нових загроз.

Перспективним напрямом подальших наукових досліджень є використання концепції Explainable Artificial Intelligence (XAI) — пояснюваного штучного інтелекту. Технології XAI спрямовані на підвищення прозорості процесу прийняття рішень нейронними мережами та надання зрозумілих пояснень щодо причин класифікації певної події як аномальної або потенційно небезпечної. Впровадження таких підходів дозволить підвищити рівень довіри до систем штучного інтелекту, спростити їх аудит та забезпечити більш ефективну взаємодію між автоматизованими засобами захисту та фахівцями з кібербезпеки.

Таким чином, подальший розвиток методів глибокого навчання пов'язаний не лише зі зростанням точності виявлення атак, але й з вирішенням проблем інтерпретованості, ресурсомісткості та адаптації моделей до динамічного середовища сучасних комп'ютерних мереж.

Наукова новизна

Наукова новизна даної роботи полягає в комплексному узагальненні сучасних підходів до застосування методів глибокого навчання для аналізу мережевого трафіку та виявлення аномальної мережевої активності в умовах сучасних кіберзагроз. У роботі проведено систематизацію основних архітектур глибоких нейронних мереж, які використовуються в системах виявлення вторгнень, а також визначено їхні переваги та особливості застосування для задач кібербезпеки.

Особливу увагу приділено порівняльному аналізу таких архітектур, як згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN), мережі довгої короткочасної пам’яті (LSTM) та автоенкодери. На основі проведеного аналізу визначено найбільш перспективні підходи до виявлення аномалій у мережевому трафіку, здатні забезпечити високу точність класифікації та ефективне виявлення як відомих, так і нових типів кібератак.

Наукова новизна також полягає у визначенні ключових факторів, що впливають на ефективність використання глибоких нейронних мереж у режимі реального часу, зокрема обсягів навчальних даних, вибору архітектури моделі, параметрів навчання та особливостей мережевого середовища. Це дозволяє сформувати рекомендації щодо підвищення якості функціонування інтелектуальних систем моніторингу мережевої безпеки.

Крім того, у роботі обґрунтовано доцільність поєднання сучасних методів глибокого навчання з технологіями пояснюваного штучного інтелекту (Explainable AI), що сприяє підвищенню прозорості процесу прийняття рішень та довіри до автоматизованих систем виявлення загроз.

Таким чином, отримані результати розширюють наукові уявлення щодо можливостей застосування глибоких нейронних мереж у сфері кібербезпеки та можуть бути використані як теоретична основа для подальшого вдосконалення систем виявлення аномальної мережевої активності в режимі реального часу.

Висновки

У результаті проведеного дослідження було проаналізовано можливості використання глибоких нейронних мереж для виявлення аномальної мережевої активності в сучасних комп’ютерних мережах. Встановлено, що стрімке зростання кількості кіберзагроз, ускладнення методів проведення атак та збільшення обсягів мережевого трафіку вимагають застосування нових інтелектуальних підходів до забезпечення інформаційної безпеки. Одним із найбільш перспективних напрямів вирішення цієї проблеми є використання технологій глибокого навчання.

У роботі було розглянуто основні архітектури глибоких нейронних мереж, які застосовуються для аналізу мережевого трафіку, зокрема CNN, RNN, LSTM та Autoencoder. Проведений аналіз показав, що кожна з цих архітектур має власні переваги залежно від характеру даних та поставлених

завдань. Водночас найбільш ефективними для виявлення аномалій у мережевому трафіку виявилися моделі LSTM та Autoencoder. Мережі LSTM демонструють високу результативність при аналізі часових послідовностей та виявленні складних закономірностей у мережевих потоках, тоді як Autoencoder ефективно виявляють відхилення від нормальної поведінки навіть за відсутності великої кількості прикладів атак під час навчання.

Дослідження підтвердило, що використання глибокого навчання дозволяє значно підвищити точність виявлення вторгнень, зменшити кількість хибних спрацьовувань та автоматизувати процес аналізу великих обсягів мережевих даних. Важливою перевагою таких систем є здатність виявляти не лише відомі, але й нові типи атак, що особливо актуально в умовах постійної еволюції кіберзагроз.

Разом із тим встановлено, що впровадження глибоких нейронних мереж супроводжується низкою проблем, серед яких висока потреба в обчислювальних ресурсах, необхідність використання великих навчальних вибірок та складність інтерпретації результатів роботи моделей. Для подолання цих обмежень перспективним напрямом є використання технологій Explainable Artificial Intelligence (XAI), які забезпечують прозорість процесу прийняття рішень та підвищують довіру до систем штучного інтелекту.

Отже, глибокі нейронні мережі є ефективним інструментом побудови сучасних систем виявлення вторгнень та аналізу мережевого трафіку. Подальший розвиток методів штучного інтелекту, удосконалення алгоритмів глибокого навчання та інтеграція пояснюваних моделей сприятимуть створенню більш надійних, адаптивних та високоточних систем кіберзахисту, здатних функціонувати в режимі реального часу та оперативно реагувати на сучасні кіберзагрози

Список використаної літератури

1. Deep Learning / Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.

2. Neural Networks and Deep Learning / Nielsen M. *Neural Networks and Deep Learning*. 2015.

3. Convolutional Neural Network / LeCun Y., Bengio Y., Hinton G. Deep Learning. *Nature*. 2015.

4. Long Short-Term Memory / Hochreiter S., Schmidhuber J. Long Short-Term Memory. *Neural Computation*. 1997.

5. Autoencoder / Hinton G., Salakhutdinov R. Reducing the Dimensionality of Data with Neural Networks. *Science*. 2006.

6. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*.

7. OWASP. OWASP Top 10 Web Application Security Risks.

8. Cisco. Annual Cybersecurity Reports.

9. IBM. X-Force Threat Intelligence Reports.

10. Kaspersky. Cyberthreat Intelligence Reports.

References

1.Deep Learning / Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.

2.Neural Networks and Deep Learning / Nielsen M. *Neural Networks and Deep Learning*. 2015.

3.Convolutional Neural Network / LeCun Y., Bengio Y., Hinton G. Deep Learning. *Nature*. 2015.

4.Long Short-Term Memory / Hochreiter S., Schmidhuber J. Long Short-Term Memory. *Neural Computation*. 1997.

5.Autoencoder / Hinton G., Salakhutdinov R. Reducing the Dimensionality of Data with Neural Networks. *Science*. 2006.

6.NIST. *Framework for Improving Critical Infrastructure Cybersecurity*.

7.OWASP. OWASP Top 10 Web Application Security Risks.

8.Cisco. Annual Cybersecurity Reports.

9.IBM. X-Force Threat Intelligence Reports.

10.Kaspersky. Cyberthreat Intelligence Reports.