les/describe-cloud-service-types/4-describe-software-service. Дата доступу: 1 квітня 2024.
[12]. "PaaS" Learn Microsoft, [електронний ресурс]. https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/3-describe-platform-service. Дата доступу: 1 квітня 2024.
[13]. "IaaS" Learn Microsoft, [електронний ресурс]. https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/2-describe-infrastructure-service. Дата доступу: 1 квітня 2024.

RESEARCH AND ANALYSIS OF PROBLEMS AND CHALLENGES IN ENSURING CYBERSECURITY IN CLOUD COMPUTING

Cloud services provide information tools in a virtual environment with the ability to expand the software and hardware resources of a user's computer device. In this case, the information is permanently stored on servers on the Internet and temporarily cached on client devices, such as personal computers, game consoles, laptops, smartphones, etc. To get constant access to remote Internet resources, users use cloud services. They are a key element of modern and rapidly developing technologies, and for many companies, the use of cloud services is a strategic issue. Although the innovative capabilities of cloud services attract the attention of users on the one hand, they can also pose new threats to their information security. That is why the study of cloud computing is important to understand its potential and effectiveness. This study will examine the security aspect of cloud services and compare several different platforms in this context, as the lack of sufficient protection can lead to theft of personal data and other confidential information. The study will also look at the most common threats faced by cloud services, such as DDoS attacks, data leaks, data misuse, etc. In particular, we will analyze the security measures provided by leading cloud platforms such as AWS, GCP and Azure to determine their effectiveness and reliability. Our analysis will be useful both for companies considering moving to the cloud and for ordinary users seeking to keep their personal data safe online. The results of the study will provide a clear picture of the benefits and limitations of using different cloud platforms from a security perspective.

Keywords: cloud services, AWS, AZURE, GCP, cyber security.

Король Марта Ярославівна, студентка кафедри захисту інформації Національного університету «Львівська політехніка».
Marta Korol, student at the Department of Information Security, Lviv Polytechnic National University.
E-mail: marta.korol.kb.2022@lpnu.ua.
Orcid ID: 0009-0002-8079-1799.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».
Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.26.18830
УДК 004.49

ВИКЛИКИ ТА МОЖЛИВОСТІ КІБЕРБЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ (IOT): ПОЄДНАННЯ ШТУЧНОГО ІНТЕЛЕКТУ, IOT ТА КІБЕРБЕЗПЕКИ

Олександр Улічев, Роман Яровий, Костянтин Задорожний

Метою роботи є дослідження викликів та можливостей, пов'язаних з кібербезпекою в контексті інтернету речей (IoT) та поєднанням штучного інтелекту (ШІ) з IoT, відомим як AIoT. Робота розглядає еволюцію IoT до AIoT, важливість кібербезпеки в AIoT та різноманітні виклики, що виникають у зв'язку зі збільшенням кількості підключених до мережі пристроїв та зростанням обсягу даних. Дослідження також розглядає стратегії кібербезпеки для AIoT, включаючи захист мережевого зв'язку, використання штучного інтелекту в системах виявлення та запобігання кібератак, контроль доступу та ідентифікацію, а також оперативний моніторинг та виявлення аномалій. В статті розглядається питання стандартизації та регулювання в галузі AIoT-кібербезпеки та майбутні напрями розвитку в цій галузі, зокрема приділено увагу напрямкам: використання блокчейн-технологій, розширення ролі штучного інтелекту в кібербезпеці AIoT. Заключна частина статті містить висновки дослідження, рекомендації щодо подальших досліджень та вдосконалення кібербезпеки в AIoT.

***Ключові слова**: інтернет речей (IoT), штучний інтелект, аномалії трафіку, штучний інтелект речей(AIoT), кібербезпека, дерева рішень, K-найближчі сусіди, машини опорних векторів.*

ВСТУП

Інтернет речей стрімко розвивається, сьогодні кількість пристроїв в мережі оцінюється десятками мільярдів – починаючи від побутових домашніх пристрої, закінчуючи агрегатами промислового виробництва та спеціальними пристроями в прикладних галузях (наука, освіта, медицина). За прогнозами електронного видання Statista [15], кількість пристроїв Інтернету речей (IoT) у світі майже подвоїться з 15,1 мільярда у 2020 році

до понад 29 мільярдів у 2030 році. Розвиток технологій, на кшталт комунікаційних технологій типу 5G і їх наступників, дозволяють втілювати в життя ідеї, що ще 10-20 років тому можна було зустріти лише на сторінках фантастичних романів. Сьогодні вже нікого не дивують «розумні холодильники», реалізуються проекти «розумних будинків», починають реалізовуватись великі проєкти «розумних міст».

Інтернет речей (IoT) вносить значний вклад у наше повсякденне життя, але водночас викликає ряд проблем з точки зору кібербезпеки. Ось деякі з викликів та можливостей, пов'язаних із кібербезпекою в інтернеті речей.

Виклики:

1. Брак стандартів безпеки: багато пристроїв IoT випускаються з недостатньою захистом і не відповідають загальноприйнятим стандартам безпеки. Це робить їх вразливими до атак;

2. Недостатня захищеність пристроїв: багато IoT-пристроїв мають обмежені ресурси, тому важко реалізувати потужні механізми захисту;

3. Низька свідомість користувачів: багато користувачів не мають належного розуміння про те, як забезпечити безпеку своїх підключених пристроїв;

4. Збільшення атак мережі: кількість підключених пристроїв швидко зростає, що робить мережу більш вразливою до різноманітних кібератак;

5. Проблеми з конфіденційністю даних: багато IoT-пристроїв збирають великі обсяги особистих даних, що може стати об'єктом порушення конфіденційності.

Можливості:

1. Розвиток стандартів безпеки: існують можливості для розробки та впровадження стандартів безпеки для IoT-пристроїв, що дозволить створити єдиний підхід до захисту;

2. Вдосконалення алгоритмів шифрування: розвиток сучасних методів шифрування допоможе забезпечити безпеку передачі інформації між пристроями та серверами;

3. Інтеграція технологій блокчейн: технології блокчейн можуть забезпечити додатковий рівень безпеки шляхом створення децентралізованих систем, які важко атакувати;

4. Освіта користувачів: підвищення рівня освіти користувачів щодо безпеки IoT-пристроїв може допомогти уникнути багатьох загроз;

5. Розробка інтелектуальних систем виявлення загроз: використання штучного інтелекту та машинного навчання для виявлення аномальних дій в мережі може допомогти реагувати на потенційні загрози.

Загальною метою є розвиток комплексних підходів до кібербезпеки в інтернеті речей, щоб забезпечити безпеку й приватність користувачів та підвищити стійкість мережі.

Зрозуміло, що будь-який новий напрямок, неодмінно супроводжується і певним набором нових проблем та викликів. На проблеми, пов’язані з розвитком та використанням інтернету речей, вказують ряд зарубіжних та вітчизняних авторів.

Зокрема, серед зарубіжних авторів, варто виділити наступних авторів. Автори статті[1] розглядають зміну парадигми в зв’язку з розвитком інтернету речей. В статтях [2,3] розглядається роль штучного інтелекту в технологіях інтернету речей та перехід до AIoT. Автори (редактори)книги «Розробка інтернету речей» [4] розглядають загальну архітектуру технології, вказують на можливі перспективи розвитку та застосування, водночас ставлять і питання пов’язані з безпекою. Безпосередньо питання безпеки детально розглядає автор D. Etter [5]. Ця книга є дослідженням найкращих стратегій впровадження безпеки IoT, в книзі описано механізми забезпечення безпеки систем Інтернету речей, на прикладі досвіду організацій, що вже запровадили та використовують технологію IoT.

Питанням правового регулювання в сфері інтернету речей присвячено ряд статей та публікацій як зарубіжних так і вітчизняних дослідників. Колодін Д. в статті[13] досліджує суспільні відносини, що виникають з приводу використання «інтернету речей», на предмет необхідності їх правового регулювання, виокремлює найбільш пріоритетні сфери, пов’язані з функціонуванням «інтернету речей», які потребують нагального правового регулювання. Серед вітчизняних авторів питанням безпеки IoT приділяють увагу Гресько А., Щебланін Ю.[10], питання безпеки також розглядають автори статті[11]. Автор Баранов О. в статті[12] розглядає можливість застосування технології блокчейн в роботі IoT.

ПОСТАНОВКА ПРОБЛЕМИ

Інтернет речей та штучний інтелект (AI) стали двома сильними технологічними трендами, які впливають на різні сфери нашого життя. Поєднання цих двох технологій в AIoT (AI of Things) відкриває безліч нових можливостей, включаючи покращену автоматизацію, аналіз даних у реальному часі та інтелектуалізацію пристроїв. Проте, разом з розширенням функціональності AIoT

виникають і суттєві проблеми кібербезпеки, які потребують відповідних рішень.

Перша проблема стосується збільшення кількості підключених пристроїв та точок доступу в AIoT. З кожним новим підключеним пристроєм зростає потенційна поверхня атаки для зловмисників. Це може стати причиною появи нових вразливостей, а також збільшити ризик неправильної конфігурації та керування системами AIoT.

Друга проблема полягає в вразливості кожного окремого пристрою та можливості атак на ці пристрої, використовуючи їх вразливості. Багато з цих пристроїв мають обмежені ресурси та обчислювальну потужність, що ускладнює реалізацію надійних механізмів безпеки. Зловмисники можуть використовувати ці вразливості для незаконного доступу до системи, розповсюдження шкідливих програм або навіть захоплення контролю над цілими мережами пристроїв.

Третя проблема пов'язана зі забезпеченням безпеки в складних AIoT-системах. AIoT включає в себе велику кількість пристроїв, мереж та різноманітних компонентів, які взаємодіють між собою. Це створює складність в управлінні та моніторингу безпеки системи, оскільки вимагає забезпечення цілісності, конфіденційності та доступності для всієї інфраструктури AIoT.

Нарешті, збільшення обсягу даних, що збираються та обробляються AIoT-системами, ставить під загрозу приватність та безпеку особистих даних. Ці дані можуть містити певну особисту інформацію або надавати шляхи отримання такої інформації, що, в свою чергу, може бути використано для шахрайства, шпигунства або шантажу. Існує потреба у розумному аналізі та захисті цих даних, щоб забезпечити конфіденційність та інтегритет інформації в AIoT-системах.

Отже, основні проблеми кібербезпеки в AIoT включають збільшення кількості підключених пристроїв, вразливості та атаки на підключені IoT-пристрої, проблеми зі забезпеченням безпеки в складних системах AIoT та ризики, пов'язані зі збиранням та обробкою великого обсягу особистих даних. Вирішення цих проблем вимагає розробки ефективних стратегій кібербезпеки, стандартизації, співпраці між країнами та використання новітніх технологій, таких як блокчейн та штучний інтелект.

ОСНОВНА ЧАСТИНА

Зміна парадигми: Інтернет речей до AIoT

В інтернеті речей ми спостерігаємо постійний розвиток та зростання. Протягом останніх років IoT виявився потужним інструментом для збирання, обробки та обміну даних між різними пристроями та системами. Однак, з появою штучного інтелекту на сцені подій настає нова ера, відома як «інтернет речей розуму» або AIoT.

Штучний інтелект речей (Artificial intelligence of things, AIoT[1]) – це поєднання технологій штучного інтелекту (AI) та інфраструктури Інтернету речей (IoT). Метою AIoT є створення більш ефективних операцій IoT, покращення взаємодії між людиною та машиною та покращення управління даними та аналітики.

Еволюція IoT до AIoT відбувається завдяки поєднанню штучного інтелекту з IoT, що веде до додаткових можливостей та складності. Штучний інтелект додає інтелектуальні функції до підключених пристроїв, дозволяючи їм здійснювати самостійне прийняття рішень, аналізувати дані, виконувати складні завдання та навіть навчатися на основі зібраних даних.

У пристроях AIoT штучний інтелект вбудовано в компоненти інфраструктури, такі як програми та набори мікросхем, які підключені за допомогою мереж IoT. Тоді API використовуються для забезпечення того, щоб усі апаратні засоби, програмне забезпечення та компоненти платформи могли працювати та спілкуватися разом без зусиль з боку кінцевого користувача.

У робочому стані пристрої IoT створюють і збирають дані, а потім штучний інтелект аналізує їх, щоб надати розуміння та підвищити ефективність і продуктивність. ШІ отримує інформацію за допомогою таких процесів, як навчання даних.

Поєднання штучного інтелекту з IoT відкриває нові розширені можливості та переваги. Наприклад, системи AIoT можуть прогнозувати та уникати виникнення проблем, виявляти аномальну поведінку, оптимізувати процеси та вдосконалювати продуктивність. Застосування штучного інтелекту дозволяє IoT-пристроям стати більш «розумними», адаптивними та ефективними.

Однак, зростання обсягу даних та потреба у розумному аналізі ставлять виклики перед кібербезпекою в AIoT-системах. Забезпечення безпеки даних, конфіденційності, цілісності та доступності стає ще більш важливим завданням. Виникають питання щодо захисту приватності користувачів, ідентифікації та автентифікації пристроїв, виявлення та запобігання кібератак, а також розробки відповідних стандартів та протоколів безпеки для AIoT.

Розширені можливості та складність AIoT відкривають нові перспективи та виклики для кібербезпеки. Є необхідність в розробці та вдос-

коналенні стратегій та методів захисту для ефективного впровадження AIoT-технологій.

Виклики кібербезпеки в AIoT

Збільшення кількості підключених пристроїв та точок доступу є одним з головних викликів у сфері кібербезпеки AIoT. Завдяки швидкому росту IoT та впровадженню штучного інтелекту, кількість підключених пристроїв стає все більшою, що вимагає забезпечення безпеки для кожного з них. Це створює потенційні точки входу для зловмисників, які можуть скористатися вразливостями пристроїв або мережі для здійснення кібератак.

Одним із найпоширеніших типів атак на IoT є атака Man-in-the-Middle (MITM)[6, 7]. Ця атака полягає у перехопленні комунікації між двома вузлами та дозволяє зловмиснику виступити як посередник. У випадку IoT, зловмисник може виконувати атаки MITM між пристроєм IoT та програмою, з якою він взаємодіє. Вразливість пристроїв IoT до атак MITM виникає з-за їхньої недостатньої захищеності та відсутності стандартних механізмів боротьби з такими атаками. Зловмисники можуть використовувати методи, такі як отруєння ARP або зміна налаштувань DNS, або перехоплювати трафік HTTPS для перенаправлення мережевого трафіку та використання даних, що передаються між пристроями, в злочинних цілях.

Поширеною формою атаки MITM проти пристроїв IoT є з'єднання Bluetooth. Багато пристроїв IoT використовують Bluetooth Low Energy (BLE), який розроблено з урахуванням пристроїв IoT, щоб бути меншими, дешевшими та енергоефективними. Однак BLE вразливий до атак MITM. BLE використовує шифрування AES-CCM; Шифрування AES вважається безпечним, але спосіб обміну ключами шифрування ні. Рівень безпеки залежить від методу та налаштувань з'єднання, що використовується для обміну тимчасовими ключами між пристроями. BLE спеціально використовує трифазні процеси сполучення: спочатку пристрій-ініціатор надсилає запит на з'єднання, а пристрої обмінюються можливостями з'єднання через незахищений канал; по-друге, пристрої обмінюються тимчасовими ключами та перевіряють, що вони використовують той самий тимчасовий ключ, який потім використовується для генерації короткострокового ключа (деякі новіші пристрої використовують довгостроковий ключ, обмін яким здійснюється за допомогою криптографії відкритого ключа Еліптичної кривої Діффі-Хеллмана, який значно безпечніший за стандартний протокол BLE);

Використання пристроїв IoT для створення ботнетів та здійснення розподілених атак на відмову в обслуговуванні (DDoS) є ще одним серйозним викликом для кібербезпеки в AIoT. Атаки DDoS мають на меті перевантажити мережеву інфраструктуру цільової служби та завадити нормальному потоку даних. DDoS-атаки зазвичай проходять кілька етапів: вербування, під час якого зловмисник шукає вразливі машини, які будуть використані в DDoS-атаці проти цілі; експлуатація та зараження, під час яких використовуються вразливі машини та впроваджується шкідливий код; спілкування, в якому зловмисник оцінює заражені машини, бачить, які з них онлайн, і вирішує, коли планувати атаки або оновлювати машини; і атака, під час якої зловмисник дає команду зараженим машинам надсилати шкідливі пакети до цілі. Одним із найпопулярніших способів є створення ботнетів, використовуючи уразливі пристрої IoT, що дозволяє їм здійснювати різноманітні типи DDoS-атак. Хробак Mirai є прикладом такої атаки, коли заражені пристрої IoT використовуються для запуску масштабних DDoS-атак. Застосування розподілених атак з використанням пристроїв IoT створює потенційну загрозу для безпеки цільових систем та мереж.

Пристрої IoT також можуть стати об'єктом атак на відмову в обслуговуванні (DoS). Атаки на постійну відмову в обслуговуванні (PDoS) спрямовані на повне зруйнування пристрою або системи. Зловмисники можуть перевантажити батарею або систему живлення пристрою, або використовувати вразливості мікропрограми для заміни основного програмного забезпечення на пошкоджену версію. Атаки на систему живлення можуть призвести до повного вичерпання ресурсів пристрою та потребувати його заміни.

Розвиток ефективних методів та стратегій кібербезпеки є критичним завданням для AIoT. Забезпечення безпеки пристроїв та мережі, виявлення та запобігання кібератак, а також захист конфіденційності та приватності особистих даних є необхідними кроками для забезпечення безпеки та стійкості AIoT-систем.

Штучний інтелект у кібербезпеці

Для динамічного захисту систем від кіберзагроз, значна кількість експертів все частіше вдається до застосування штучного інтелекту (ШІ). Ця передова технологія використовується переважно для виявлення вторгнень у кіберпросторі

шляхом аналізу моделей трафіку та виявлення активностей, які є характерними для атаки.

Одним з основних етапів ефективного застосування ШІ є навчання системи. Існують два основних види машинного навчання: контрольоване та неконтрольоване. Контрольоване навчання передбачає, що люди вручну позначають навчальні дані як «правильні» або «неправильні» (в залежності від критеріїв, параметрів та видів задач), а потім вводять ці дані в алгоритм для створення моделі з «класами» даних, які порівнюються з трафіком, що він аналізує. Неконтрольоване навчання відмовляється від тренувальних даних та ручного маркування, замість цього алгоритм автоматично групує схожі частини даних у класи та класифікує їх згідно з узгодженістю даних всередині класу та відмінності між класами. Один із популярних алгоритмів машинного навчання для кібербезпеки - це наївний алгоритм Баєса. Цей алгоритм прагне класифікувати дані на основі теореми Баєса, припускаючи, що всі аномальні дії походять від незалежних подій, а не від одного типу атаки. Наївний баєсів класифікатор є контрольованим алгоритмом навчання, і після того, як він навчений та сформував свої класи, аналізуватиме кожну дію, щоб визначити ймовірність того, що вона є аномальною. Алгоритми машинного навчання також можуть використовуватись для створення інших моделей, про які йдеться у цій частині статті.

Дерева рішень[8,9]. Дерево рішень - це тип штучного інтелекту, який створює набір правил на основі навчальних зразків даних. Дерево використовує ітеративний поділ для знаходження опису (часто просто «атака» або «нормальний стан»), який найкращим чином категоризує трафік, що аналізується.

Прикладом такого підходу у кібербезпеці є виявлення атак DoS за допомогою аналізу швидкості потоку, розміру та тривалості надходження трафіку. Наприклад, якщо швидкість потоку низька, але тривалість трафіку довга, ймовірно, що це атака, і вона буде відповідно класифікована. Дерева рішень також можуть використовуватись для виявлення атак командної ін'єкції на роботизованих транспортних засобах, класифікуючи значення з використання ЦП, потоку мережі та обсягу записаних даних. Цей підхід є досить популярним, оскільки, в більшості випадків, інтуїтивно зрозуміло - які типи трафіку вважати аномальними. Крім того, якщо знайдено ефективний набір правил, штучний інтелект може аналізувати трафік в реальному часі, надаючи практично миттєве сповіщення у разі виявлення незвичайної активності.

Ще одним підходом з використанням дерев рішень є техніка вивчення правил (Rule-Learning), яка шукає набір характеристик атаки на кожній ітерації, максимізуючи певний показник, що позначає якість класифікації (тобто кількість неправильно класифікованих зразків даних). Основна відмінність між традиційними деревами рішень та технікою вивчення правил полягає в тому, що традиційні дерева рішень шукають характеристики, які призводять до класифікації, тоді як техніка вивчення правил знаходить повний набір правил, що можуть описати клас. Це може бути перевагою, оскільки при формуванні правил можна враховувати поради експертів, що дозволяє створити оптимізований набір правил.

К-найближчі сусіди (k-nearest neighbor , k-NN). Техніка к-найближчі сусіди (k-NN) вивчає зразки даних, щоб створити класи, аналізуючи евклідову відстань між новим фрагментом даних та вже класифікованими фрагментами даних, щоб визначити, до якого класу слід віднести новий фрагмент. Експерти з кібербезпеки також досліджують застосування к-найближчих сусідів для виявлення кібератак у реальному часі. Ця техніка застосовується для виявлення атак, таких як атаки внесення хибних даних, і показує високу ефективність, у випадку, коли дані представлені за допомогою моделей, що дозволяє вимірювати їх відстань до інших даних, використовуючи розподіл Гауса або вектор.

Машини опорних векторів (Support Vector Machines, SVM). Машини опорних векторів є розширенням моделей лінійної регресії, які розміщують площину, що розділяє дані на два класи. Ця площина може бути лінійною, нелінійною, поліноміальною, гаусовою, сигмоподібною, залежно від функції, яка використовується в алгоритмі. SVM також можуть розділяти дані на більш, ніж два класи, використовуючи більше однієї площини. У кібербезпеці ця техніка використовується для аналізу шаблонів інтернет-трафіку та розділення їх на компонентні класи, такі як HTTP, FTP, SMTP тощо. Оскільки SVM є технікою контрольованого машинного навчання, його часто використовують у застосунках, де можуть бути симульовані атаки, наприклад, використовуючи мережевий трафік, згенерований під час тестування на проникнення, як тренувальні дані.

Штучні нейронні мережі (ШНМ, Artificial Neural Networks, ANNs). ШНМ – це техніка, за-

снована на типі взаємодії нейронів один з одним для передачі та інтерпретації інформації. У штучних нейронних мережах нейрон є математичним рівнянням, яке отримує на вхід дані та видає цільове значення, інформація передається наступному нейрону, з урахуванням його значення. Алгоритм ШНМ ітеративно виконується до тих пір, поки значення виходу не стане достатньо близьким до цільового значення, що дозволяє нейронам вчитися та коригувати свої вагові коефіцієнти, шляхом вимірювання похибки між очікуваним значенням та попереднім вихідним значенням. Після завершення цього процесу алгоритм представляє математичне рівняння, яке видає значення, що можна використовувати для класифікації даних.

Величезною перевагою штучних нейронних мереж є їх здатність адаптувати математичні моделі при представленні нової інформації, тоді як інші математичні моделі можуть застаріти, коли нові типи трафіку та атак стають загальними. Це також означає, що ШНМ добре впораються з розпізнаванням раніше невидимих атак та атак нульового дня, оскільки вони більше враховують нову інформацію, ніж статичні математичні моделі. Завдяки цьому штучні нейронні мережі є надійними системами виявлення вторгнень і успішно справляються з атаками, такими як DoS.

На даний момент використання ШІ в кібербезпеці є досить обмеженим, але напрямок швидко розвивається. Застосування ШІ вимагає великих грошових та ресурсних затрат, тому використання ШІ для захисту невеликої системи може бути недоцільним. Однак компанії, які мають великі мережі, можуть отримати переваги від таких рішень, особливо якщо розглядають або вже впровадили пристрої Інтернету речей в свою мережу. Кібербезпека з використанням штучного інтелекту також може бути корисною в розумних містах з величезними системами, де штучний інтелект зможе забезпечити дуже швидкий час реакції, що важливо для систем глобальних керованих систем, наприклад - управління міським рухом. У майбутньому кібербезпека з використанням штучного інтелекту також може бути інтегрована й в менші системи, такі як автономні автомобілі чи розумні будинки.

Розробка стратегій кібербезпеки для AIoT

Розробка ефективних стратегій кібербезпеки є ключовим аспектом для забезпечення безпеки AIoT-систем. У цьому пункті розглядатиметься декілька важливих аспектів, які включаються до таких стратегій. Забезпечення захищеної комунікації. Забезпечення захищеної комунікації в AIoT вимагає використання потужних протоколів шифрування та аутентифікації для захисту даних під час їх передачі по мережі. Один із таких протоколів це TLS (Transport Layer Security): TLS є широко використовуваним протоколом, який забезпечує захищену передачу даних між пристроями у мережі. Він використовує шифрування для захисту конфіденційності даних та механізми аутентифікації для перевірки ідентичності комунікуючих сторін. Наступний протокол це IPSec (Internet Protocol Security): IPSec забезпечує захищену передачу даних на рівні IP-пакетів. Він використовує шифрування та механізми аутентифікації для забезпечення безпеки трафіку між пристроями. MQTT (Message Queuing Telemetry Transport) з TLS: MQTT є легковагим протоколом для комунікації IoT-пристроїв. Використання TLS разом з MQTT дозволяє забезпечити захищений канал зв'язку між сенсорами, датчиками та центральною системою. Виявлення та відповідь на аномальну активність. Для виявлення та реагування на аномальну активність в AIoT застосовують ряд алгоритмів машинного навчання та інтелектуальних систем:

1. K-Means Clustering: K-Means Clustering - це алгоритм машинного навчання без контролю, який кластеризує точки даних у окремі групи. Він використовується для виявлення аномалій шляхом відокремлення точок даних, які не вписуються в один кластер;

2. Ізольовані ліси: ізольовані ліси – це алгоритм машинного навчання без контролю, який працює шляхом ізоляції окремих точок даних і формування ансамблю дерев рішень. Алгоритм здатний виявляти аномалії на основі того, скільки часу потрібно для розділення точок даних;

3. Машини опорних векторів. Машини опорних векторів - це керовані алгоритми машинного навчання, які використовують математичну функцію для класифікації точок даних. Вони використовуються для виявлення аномалій шляхом визначення точок даних, які знаходяться далеко від загального набору даних;

4. Нейронні мережі. Нейронні мережі – це тип керованого алгоритму машинного навчання, який використовує кілька рівнів вузлів для обробки даних. Вони використовуються для виявлення аномалій шляхом виявлення шаблонів і кореляцій, які не відповідають очікуваній поведінці.

Забезпечення доступу та ідентифікації. Для забезпечення безпеки доступу та ідентифікації в AIoT можуть бути використані такі механізми:

а) двофакторна аутентифікація: вимагання введення не тільки пароля, але і додаткового ідентифікаційного елементу, наприклад, SMS-коду або відбитку пальця, забезпечує більший рівень безпеки;

б) використання цифрових сертифікатів: завантаження та використання цифрових сертифікатів дозволяє перевіряти автентичність пристроїв та користувачів у мережі;

в) ролева модель доступу: використання ролей та прав доступу дозволяє обмежувати доступ користувачів та пристроїв до конкретних ресурсів у системі;

г) біометрична ідентифікація: використання біометричних даних, таких як розпізнавання обличчя або сканування відбитків пальців, може забезпечити надійну ідентифікацію користувачів.

Ці стратегії та механізми кібербезпеки повинні бути інтегровані в різні аспекти AIoT системи, починаючи від розробки пристроїв і закінчуючи впровадженням програмного забезпечення та рішень. Регулярні оновлення та аудит безпеки також грають важливу роль у забезпеченні сталої кібербезпеки AIoT систем у змінних умовах загроз. Крім того, залучення фахівців з кібербезпеки та використання сучасних аналітичних інструментів допомагають швидко виявляти та вирішувати потенційні інциденти безпеки. З цими заходами можна забезпечити надійний та стійкий рівень кібербезпеки для AIoT, забезпечуючи безпечну та надійну експлуатацію інтернету речей у сучасному світі.

Стандартизація та регулювання в галузі AIoT-кібербезпеки

З розвитком технологій ШІТ та ШІ, стає очевидним, що стандартизація кібербезпеки в галузі AIoT є надзвичайно важливим аспектом для забезпечення безпеки та захищеності систем. За відсутності стандартів, інтернет речей та штучний інтелект можуть стати легкими мішенями для зловмисників, оскільки ці технології є вразливими до різноманітних кібератак. Стандартизація дозволяє створити єдиний набір правил, протоколів та норм, які дотримуються виробники, розробники, адміністратори мереж та користувачі. Це сприяє забезпеченню високого рівня кібербезпеки, співпраці різних пристроїв та систем, а також захисту конфіденційності, цілісності та доступності даних.

Організації та ініціативи зі стандартизації AIoT-кібербезпеки. Декілька міжнародних організацій та ініціатив працюють над розробкою стандартів кібербезпеки в галузі AIoT:

1. Міжнародна організація зі стандартизації (ISO):

- ISO/IEC 27000: описує мету системи управління інформаційною безпекою (ISMS), системи управління, схожої за концепцією на рекомендовані іншими стандартами ISO, такими як ISO 9000 та ISO 14000 , яка використовується для управління ризиками інформаційної безпеки та засобів контролю в організації;
- ISO/IEC 27001: встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації;
- ISO/IEC 27002: описує настанови щодо організаційної безпеки інформації та практики управління інформаційною безпекою;
- ISO/IEC 30141: визначає стандарти, характеристики та моделі для чітко визначеної та функціональної архітектури IoT;
- ISO/IEC 15408: встановлює загальні принципи оцінки безпеки IT;
- ISO/IEC 27005: містить настанови щодо управління ризиками інформаційної безпеки;
- ISO/IEC 27017: надає вказівки щодо засобів контролю інформаційної безпеки, застосовних до використання хмарних служб;
- ISO/IEC 27018: визначає персональних даних в хмарних обчисленнях, що надаються службами персональної інформації;
- ISO/IEC 18028: надає детальні вказівки щодо аспектів безпеки керування, експлуатації та використання мереж інформаційних технологій (IT) та їх взаємозв'язків;
- ISO/IEC 27035: представляє основні концепції, принципи та процеси з ключовими діями управління інцидентами інформаційної безпеки, які забезпечують структурований підхід до підготовки, виявлення, звітування, оцінки та реагування на інциденти, а також застосування отриманих уроків;
- ISO/IEC 27036: містить огляд настанов, спрямованих на допомогу організаціям у захисті їх інформації та інформаційних систем у контексті відносин з постачальниками;
- ISO/IEC 19086: прагне створити набір загальних будівельних блоків хмарних SLA (концепцій, термінів, визначень, контекстів), які можна використовувати для створення хмарних угод про рівень обслуговування (SLA);

2. Консорціум Hyperledger: Цей консорціум розробляє стандарти забезпечення кібербезпеки в

галузі блокчейну, що можуть бути застосовані для захисту та автентифікації даних в AIoT системах;

3. AllSeen Alliance: захищеність та приватність даних є одними з основних принципів роботи цієї ініціативи, яка пропонує стандарти для забезпечення безпеки в мережах IoT та AIoT.

Майбутні напрями розвитку AIoT-кібербезпеки

З прогресом технологій AIoT постають нові виклики і можливості для розвитку кібербезпеки. Деякі з майбутніх напрямів розвитку AIoT-кібербезпеки включають:

1. Використання блокчейн-технологій для забезпечення безпеки в AIoT: блокчейн-технологія може виконувати важливу роль у забезпеченні безпеки в AIoT-системах. Вона забезпечує децентралізовану та недоступну до модифікації систему обліку, яка може бути використана для підтвердження автентичності та цілісності даних, а також для забезпечення безпеки транзакцій та обміну даними між різними пристроями AIoT. Впровадження блокчейн-технологій в AIoT може допомогти вирішити проблеми, пов'язані з безпекою, такі як викрадення даних, підроблення та злам систем;

2. Розширення ролі штучного інтелекту в кібербезпеці AIoT: штучний інтелект має великий потенціал у поліпшенні кібербезпеки AIoT. Алгоритми машинного навчання та аналізу даних можуть виявляти вразливості, розпізнавати та прогнозувати кібератаки, а також реагувати на них в реальному часі. Застосування штучного інтелекту для автоматичного виявлення загроз та побудови реактивних механізмів може значно збільшити ефективність кібербезпеки в AIoT-системах;

3. Автоматизація та самоналаштування систем безпеки в AIoT: з уведенням AIoT стає складніше керувати та підтримувати безпеку систем. Тому автоматизація та самоналаштування систем безпеки є одним з важливих напрямів розвитку. Системи безпеки AIoT можуть використовувати алгоритми машинного навчання та штучного інтелекту для постійного моніторингу, виявлення аномалій та автоматичного реагування на потенційні загрози безпеки. Це дозволяє забезпечити протидію кібератакам в реальному часі та швидко адаптувати системи до нових загроз.

Розвиток цих напрямків у кібербезпеці AIoT має великий потенціал для забезпечення безпеки та стійкості цих складних систем. Використання блокчейн-технологій, розширення ролі штучного інтелекту та автоматизація систем безпеки можуть стати ключовими факторами у забезпеченні надійного та безпечного функціонування AIoT-систем у майбутньому.

ВИСНОВКИ

В статті були розглянуті виклики та можливості кібербезпеки в інтернеті речей (AIoT) - поєднанні штучного інтелекту, IoT та кібербезпеки. Виявлено, що розвиток AIoT відкриває нові перспективи та можливості, проте, зростаюча кількість підключених пристроїв також вносить нові виклики та загрози в галузі кібербезпеки. Забезпечення безпеки в інтернеті речей стає надзвичайно важливим завданням для забезпечення захищеної та надійної інфраструктури.

Одним із головних викликів є недостатня безпека та вразливість багатьох IoT-пристроїв робить їх легкою мішенню для кібератак. Швидкий ріст IoT та розширення штучного інтелекту сприяють зростанню обсягу особистих даних, що потребують надійного захисту від несанкціонованого доступу.

Використання штучного інтелекту в кібербезпеці дозволяє виявляти загрози та кібератаки швидше та точніше. Машинне навчання, рішення на основі правил, метод ближніх сусідів та інші техніки AI забезпечують аналіз великих обсягів даних та автоматичне реагування на нові вектори атак.

Для забезпечення кібербезпеки в інтернеті речей необхідно застосовувати потужні протоколи для захищеної комунікації, такі як SSL/TLS. Застосування механізмів автентифікації та авторизації допомагає контролювати доступ до систем і обмежувати привілеї користувачів. Крім того, шифрування даних, контроль доступу та аудит активності є важливими складовими для забезпечення безпеки в AIoT системах.

Важливим аспектом є стандартизація та регулювання в галузі AIoT-кібербезпеки. Робота над стандартами, спрямованими на захист IoT та систем із застосуванням штучного інтелекту, допомагає створювати єдині та сумісні рішення для різних виробників та платформ. Організації, такі як IEEE, IETF, NIST, Hyperledger та інші, активно працюють над стандартами кібербезпеки в IoT-сфері, допомагаючи зробити інтернет речей більш безпечним та захищеним.

Усі ці заходи спрямовані на забезпечення надійного та безпечного функціонування інтернету речей у майбутньому. Виклики кібербезпеки в AIoT вимагають постійної уваги та зусиль від бізнесу, науковців та урядових структур для забезпечення захищеної та стійкої інфраструктури IoT з використанням штучного інтелекту та су-

часних технологій кібербезпеки. Лише через спільні зусилля та використання передових методів кібербезпеки можемо забезпечити безпечне та успішне впровадження інтернету речей у різних сферах життя.

Майбутні напрями розвитку AIoT-кібербезпеки включають використання блокчейн-технологій для забезпечення безпеки в AIoT, розширення ролі штучного інтелекту у кібербезпеці AIoT та автоматизацію та самоналаштування систем безпеки. Ці напрями можуть значно покращити безпеку AIoT-систем та забезпечити високий рівень захисту від кіберзагроз.

Загалом, розвиток AIoT відкриває широкі можливості, але разом з тим ставить перед нами виклики у сфері кібербезпеки. Для ефективного захисту AIoT-систем потрібні комплексні стратегії, стандартизація та співпраця між країнами. Такі заходи дозволять нам забезпечити безпеку, приватність та стійкість цих розумних технологій у майбутньому.

ЛІТЕРАТУРА

[1]. Kah Phooi Seng, Li Minn Ang Ericmoore Ngharamike Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks, International Journal of Distributed Sensor Networks Volume 18, Issue 3 March 12, 2022.

[2]. Fragkos G, Tsiropoulou EE, Papavassiliou S. Artificial intelligence enabled distributed edge computing for Internet of Things applications. In: Proceedings of the 2020 16th international conference on distributed computing in sensor systems (DCOSS), Marina del Rey, CA, 25–27 May 2020, pp.450-457. New York: IEEE.

[3]. Foukalas F, Tziouvaras A. Edge AI for industrial IoT applications. IEEE Ind Electr Mag *2021*; 15: pp. 28-36.

[4]. Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things/Berlin, Springer Berlin Heidelberg, 2011.

[5]. Etter, David. IoT Security: Practical Guide Book. N.p., CreateSpace Independent Publishing Platform, 2016.

[6]. Mitnick, Kevin D., and Simon, William L. The Art of Deception: Controlling the Human Element of Security. Германия, Wiley, 2011.

[7]. Stallings, William. Network Security Essentials: Applications and Standards. Великобритания, Pearson, 2016.

[8]. Rokach, Lior, and Maimon, Oded Z. Data Mining with Decision Trees: Theory and Applications. Сингапур, World Scientific, 2008.

[9]. Louppe G. Understanding Random Forests: From Theory to Practice, PhD dissertation, University of Liège Faculty of Applied Sciences Department of Electrical Engineering & Computer Science, 2014.

[10]. Гресько А. О., Щебланін Ю. М. Загальний, комплексний опис проблем інформаційної безпеки в Інтернеті речей [Архівовано 21 січня 2022 у Wayback Machine.] //Сучасний захист інформації. 2016. №. 1. С. 69-73.

[11]. Опірський І. Р., Головчак Р. В., Мойсійчук І. Р., Балянда Т. С., Гаранюк С. П., «Проблеми та загрози безпеці IoT пристроїв» Кібербезпека: освіта, наука, техніка. № 3(15). С. 85-92. 2022

[12]. Баранов О.А. Інтернет речей (IoT) і блокчейн "Інформація і право" № 1(24)/2018 59 УДК 002.6:004:340.1.

[13]. Колодін Д.О. «Деякі правові аспекти запровадження інтернету речей»// Часопис цивілістики. 2019. Випуск 33. С. 83-86.

[14]. Бортник К.Я., Ольшевський О.В., Пащук В.Ю. Інтернет речей та як він змінить наше життя у майбутньому. Комп'ютерно-інтегровані технології: освіта, наука, вир-во. 2018. № 30/31. С. 14-18.

[15]. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide (дата звернення: 22.01.2024).

CYBERSECURITY CHALLENGES AND OPPORTUNITIES IN THE INTERNET OF THINGS (IOT): COMBINING ARTIFICIAL INTELLIGENCE, IOT AND CYBERSECURITY

The aim of the paper is to explore the challenges and opportunities related to cyber security in the context of the Internet of Things (IoT) and the combination of artificial intelligence (AI) with IoT, known as AIoT. The work examines the evolution of IoT to AIoT, the importance of cybersecurity in AIoT, and the various challenges that arise from the increasing number of networked devices and the growth of data. The study also examines cybersecurity strategies for AIoT, including network communication protection, the use of artificial intelligence in cyber-attack detection and prevention systems, access control and identification, and operational monitoring and anomaly detection. The article examines the issue of standardization and regulation in the field of AIoT cybersecurity and future directions of development in this field, in particular, attention is paid to the following areas: the use of blockchain technologies, the expansion of the role of artificial intelligence in AIoT cybersecurity. The final part of the article contains the conclusions of the study, recommendations for further research and improvement of cyber security in AIoT.

Keywords: Internet of Things (IoT), artificial intelligence, traffic anomalies, artificial intelligence of things (AIoT), cyber security, decision trees, K-nearest neighbors, support vector machines.

Улічев Олександр Сергійович, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.

Oleksandr Ulichev, candidate of technical sciences, senior lecturer of the department of cyber security and software of the Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.
E-mail: askin79@gmail.com.
Orcid ID: 0000-0003-3736-9613.

Яровий Роман Олександрович, кандидат технічних наук, доцент кафедри КНПІ, декан ФІСТ, Європейський університет, Київ, Україна.

Roman Yarovy, candidate of technical sciences, associate professor of the Department of National Institute of Scientific Research, dean of FIST, European University, Kyiv, Ukraine.
E-mail: roman.yaroviy@e-u.edu.ua.
Orcid ID: 0000-0001-8978-8137.

Задорожний Костянтин Олександрович, студент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.

Kostyantyn Zadorozhny, student of the Department of Cyber Security and Software at the Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.
E-mail: kostazadoroznij9@gmail.com.
Orcid ID: 0000-0002-5278-9627.

DOI: 10.18372/2410-7840.26.18831
УДК 004.932.2

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ КОНКАТЕНОВАНИХ ВЕКТОРІВ ВИЗНАЧЕННЯ ОСОБИ

Денис Ханін, Віктор Отенко

У епоху цифрової автентифікації системи верифікації особи за обличчям стали ключовим елементом безпеки у різних застосуваннях. Це дослідження розглядає синергію ефективності конкатенованих векторів для покращення точності біометричної автентифікації. З використанням набору даних «Celebrities in Frontal-Profile dataset» (CFP) ми досліджуємо, чи може злиття векторів, згенерованих такими моделями, як VGG-Face, Facenet, OpenFace, ArcFace та SFace, призвести до більш надійного процесу автентифікації. Методика включає обчислення відстані L2 між нормалізованими конкатенованими векторами вхідного образу обличчя та якоря, тим самим визначаючи справжність особи. Експерименти розроблені для порівняння ефективності векторів окремих моделей проти конкатенованих векторів, використовуючи такі метрики, як точність, рівень помилкових допусків (FAR) та рівень помилкових відмов (FRR). Висновки цього дослідження можуть істотно сприяти розвитку більш безпечних і надійних систем верифікації особи за допомогою використання декількох існуючих моделей без необхідності нових досліджень архітектур, їхнього проектування та навчання.

***Ключові слова**: верифікація обличчя, біометрична автентифікація, нейронні мережі, конкатеновані вектори.*

ВСТУП

У сучасному цифровому ландшафті системи верифікації обличчя [1] стали ключовими у забезпеченні безпеки та автентичності індивідуальних ідентичностей у різних застосуваннях, від безпеки мобільних пристроїв до контролю доступу в чутливих середовищах. Впровадження технології розпізнавання облич стимульоване її нетравматичністю та унікальними, важко-імітуваними характеристиками людського обличчя, що позиціонує її як лідера серед методів біометричної автентифікації.

Це дослідження розглядає потенціал покращення точності верифікації обличчя за допомогою конкатенованих векторів з декількох моделей нейронних мереж [2]. Використовуючи набір даних CFP [3], ми прагнемо визначити, чи може інтеграція векторів різних моделей створити більш надійну та безпечну систему біометричної автентифікації. Досліджуючи синергію ефективності цих конкатенованих векторів у порівнянні з векторами окремих моделей, це дослідження прагне сприяти розробці більш передових і надійних технік верифікації обличчя з використанням існуючого набору моделей для верифікації обличчя.

Еволюція технологій біометричної автентифікації значною мірою зумовлена прогресом у галузі машинного навчання та глибокого навчання [4], зокрема у сфері розпізнавання облич. Моделі нейронних мереж, такі як VGG-Face, Facenet, OpenFace, ArcFace та SFace, становлять передові напрямки досліджень та розробок у цій галузі. Ці моделі призначені для витягування та аналізу рис обличчя [5] із зображень, перетворюючи їх у числові представлення, відомі як вектори. Ці векто-