Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

Матеріали наукової онлайн-конференції "Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY

Єлизавета Литюга, студентка
Сумський державний університет, Україна

Поява напряму боротьби з кібератаками виникла через загрози, пов'язані з розвитком Інтернету, а також зростаючого обсягу даних у мережі. Вважається, що дав поштовх до розвитку інцидент 2017 року: під час атаки програми-вимагача WannaCry постраждало понад 200 000 комп'ютерів зі 150 країн. Останніми роками кількість подібних програм і ступінь завданих ними збитків стрімко зростає. У зв'язку з цим комерційні та базові інфраструктури стикаються з підвищеними ризиками витоку даних із супутніми фінансовими втратами.

Зі зростанням кіберзагроз і загроз безпеці в цифровому середовищі важливість ролі штучного інтелекту в кібербезпеці стає дедалі очевиднішою. Автоматичне виявлення інцидентів, аналіз великих обсягів даних, прогнозування потенційних вразливостей - все це є сферою застосування штучного інтелекту в кібербезпеці. Це дає змогу ідентифікувати та відбивати атаки швидше, ніж це можливо для людини. Розглянемо кілька аспектів успішного застосування адаптивних моделей у сфері кібербезпеки:

– адаптивні моделі дозволяють створювати персоналізовані стратегії безпеки. Вони здатні враховувати

– особливості кожної організації, аналізувати її інфраструктуру та історичні дані щодо атак для створення найбільш ефективних заходів безпеки.

– штучний інтелект не тільки зменшує кількість успішних кібератак, а й істотно полегшує робоче навантаження на фахівців у галузі кібербезпеки, звільняючи їхні ресурси для зосередження на інших ключових завданнях.

– штучний інтелект може бути використаний для розробки сильних систем протидії фішингу та шкідливому програмному забезпеченню.

– штучний інтелект може використовуватися для розробки системи моніторингу, яка аналізує активність у мережі та ідентифікує будь-які підозрілі дії.

З появою нових методів атак або зміною поведінки шкідливих програм адаптивні моделі швидко реорганізують свої алгоритми для виявлення цих нових загроз.

Моделі на основі штучного інтелекту мають здатність до контекстного аналізу. Це охоплює аналіз поведінки користувачів, тенденції загроз у

конкретній галузі та особливості системи безпеки організації. Ще однією важливою перевагою адаптивних моделей є те, що вони можуть аналізувати великі обсяги інформації, виділяючи з неї ключові особливості, пов'язані з потенційними загрозами.

Підвищення ефективності алгоритмів штучного інтелекту в кібербезпеці не залишається непоміченим зловмисниками. Разом зі збільшенням кількості відомих вразливостей і дефектів безпеки систем, що реєструються в бібліотеці CVE (Common Vulnerabilities and Exposures), спостерігається зростання застосування технологій штучного інтелекту для створення більш складних кібератак.

Загальна кількість вразливостей, зафіксованих у базі CVE за 2023 рік, досягла 28,961 випадків. Така цифра є рекордною і свідчить про те, що потенціал для розроблення та проведення кібератак, зокрема, заснованих на штучного інтелекту, продовжує розширюватися (CVE (Common Vulnerabilities and Exposures), Metrics, 2024).

Таблиця 1. Статистика вразливостей зафіксованих в бібліотеці CVE (Common Vulnerabilities and Exposures) на період з 2014 по 2023 рік.

Кількість вразливостей	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Загалом	228,96	225,05	220,16	118,37	117,30	116,51	114,64	66,45	66,49	77,94

Джерело: CVE (Common Vulnerabilities and Exposures), Metrics, 2024

Атаки за допомогою систем штучного інтелекту здебільшого пов'язані з плутаниною в базовій моделі машинного навчання і зломом захисту. Наприклад, генеративні змагальні мережі (різновид штучних нейронних мереж) можуть обдурити систему розпізнавання обличь. До того ж такі мережі використовують для атаки на мовні додатки та голосові біометричні системи. Варто також зазначити, що, обдуривши систему штучного інтелекту, шкідливий файл може бути помилково класифікований як безпечний. Тож, можливість атаки на алгоритми штучного інтелекту та спотворення даних може спричинити серйозні наслідки. Такі ризики вимагають розроблення додаткових методів захисту та забезпечення надійності самого штучного інтелекту.

Незважаючи на значні переваги адаптивних моделей, вони також пов'язані з низкою обмежень і викликів, які необхідно враховувати під час їх застосування. Одним з основних викликів є брак якісних даних для навчання. Для ефективної роботи адаптивних моделей потрібен великий обсяг різноманітних даних про кібератаки і загрози. Однак, часто такі дані виявляються обмеженими через конфіденційність або складність їхнього збору.

Наразі кілька інструментів ШІ використовують для розширення можливостей і автоматизації процесу виявлення та запобігання загрозам. Двома найбільш вражаючими з них є Microsoft Security Copilot і платформа Complete Cloud Email Security компанії Tessian. Крім цих двох, іншими інструментами штучного інтелекту для виявлення і запобігання атакам є Cylance, Cybereason і McAfee MVISION. У майбутньому дедалі більше компаній будуть вкладати ресурси в сполучення ШІ з наявними інструментами виявлення і запобігання.

Наразі Microsoft Security Copilot є лідером у галузі з використання штучного інтелекту для автоматичного реагування на інциденти. Однак дедалі більшої популярності набирає інструмент Darktrace. Цей інструмент кібербезпеки побудований на основі безперервного циклу зворотного зв'язку, керованого штучного інтелекту, який приймає вхідні дані ШІ і видає результати ШІ для захисту корпоративних даних від складних кібератак. Антивіруси та засоби виявлення шкідливого ПЗ, як-от Malwarebytes і Kaspersky's Endpoint Security, використовують штучного інтелекту та машинне навчання для точної ідентифікації шкідливих програм, визначення їхньої поведінки та автономного навчання новим методам обходу. Водночас такі плагіни, як BinNet AI, інтегрують ШІ з наявними платформами реверс-інжинірингу, щоб аналітики могли глибше зрозуміти двійковий машинний код із семантичної та синтаксичної точок зору.

Найпопулярніший інструмент штучного інтелекту для вивчення кібербезпеки - ChatGPT від OpenAI. Цей генеративний чат-бот зі штучним інтелектом приймає запитання користувачів, обробляє їх і дає докладні відповіді, використовуючи найсвіжішу інформацію. Він дає змогу вести бесіду в людському стилі та дізнаватися про будь-яку тему кібербезпеки. Можна використовувати власні чат-боти, звані Security GPTs (Generative Pre-Trained Transformers), щоб сфокусувати навчання на конкретних темах.

Нещодавнє опитування головних фахівців CISO з інформаційної безпеки показало такі результати, щодо впровадження ШІ в сферу інформаційної безпеки (Splunk, The CISO Report, Consulted: March, 2024):

– 70 % респондентів вважають, що штучний інтелект дає більше переваг зловмисникам, аніж захисникам, проте 35 % уже експериментують із ним з метою кіберзахисту.

– 83 % респондентів заплатили зловмисникам після атаки ransomware, чи то безпосередньо, чи то через кіберстрахування, чи то за допомогою парламентера.

– 35 % респондентів CISO вже використовують штучний інтелект для забезпечення безпеки.

– 61 % респондентів, ймовірно, будуть використовувати його в найближчі 12 місяців.

– 86 % респондентів вважають, що генеративний штучний інтелект усуне прогалини в навичках безпеки і брак кадрів.

– 96 % респондентів стали жертвами атаки вимагачів за останній рік. Більше половини респондентів заплатили понад 100 000 доларів як викуп.

Отже, взаємодія між штучного інтелекту та людьми стає ключовим фактором для забезпечення кібербезпеки в нашому цифровому суспільстві. Роль штучного інтелекту в кібербезпеці невід'ємна в сучасному цифровому суспільстві. Цей інноваційний засіб дає змогу посилювати захист від кіберзагроз, але також ставить нові виклики, які потребують уваги до аспектів безпеки та етики.

Загалом, адаптивні моделі на основі штучного інтелекту є надійним і ефективним інструментом у боротьбі з сучасними кіберзагрозами. З їхньою допомогою організації можуть підвищити свою кібербезпеку і захистити критично важливі дані від можливих атак.

Список використаних джерел

1. CVE (Common Vulnerabilities and Exposures), Metrics, 2024. URL: https://www.cve.org/About/Metrics

2. Splunk, The CISO Report, Consulted: March, 2024. URL: https://www.splunk.com/en_us/campaigns/ciso-report.html