Тому метою України зараз є посилення кіберзахисту, захист прав і свобод громадян, державних інтересів. Нашою країною були ратифіковані відповідні міжнародні угоди, створена юридична база для запуску та функціонування системи кіберзахисту. Для її вдосконалення слід розширювати міжнародну співпрацю, запозичувати корисний досвід, об'єднувати зусилля. Напрямом подальшої роботи є конкретизація Стратегії кібербезпеки України, розробка додаткових нормативно-правових актів, швидка координація дій компетентних органів. Система кіберзхисту має загальнодержавний характер, включаючи декілька напрямків: міжнародний, політичний, юридичний, організаційний, освітній.

Список використаних джерел:

1. Бакалінська О., & Бакалінський О. Правове забезпечення кібербезпеки в Україні. Піприємництво, господарство і право, 2019. 9, 100-108. https://doi.org/10.32849/2663-5313/2019.9.17

2. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ, 2016. 26(8), 327-337. https://doi.org/10.15421/40260850

3. Трофименко О., Прокоп Ю., Логінова Н., & Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації, 2019. 150-157.https://doi.org/10.18372/2410-7840.21.13951

Савчин Євгенія Андріївна
Студентка н.гр. 117 СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

РОЛЬ «ШІ» У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Штучний інтелект і кібербезпека стають все важливішими в сучасному світі, де кількість кібератак постійно зростає.

Особи, які відповідають за прийняття рішень у різних сферах, зосереджують увагу на аналізі та поліпшенні кібербезпеки. Але це не просте завдання, оскільки треба забезпечити баланс між захистом особистих даних і відповідністю нормативам.

Інновації в галузі кібербезпеки постійно розвиваються, але разом з ними розвиваються й кіберзлочинці, шукаючи нові способи атак. У такому динамічному середовищі кібербезпека стає набагато важливішою, ніж раніше.

Штучний інтелект і кібербезпека йдуть пліч-о-пліч, оскільки ми дивимося в цифрове майбутнє і використовуємо новітні технології, щоб залишатися захищеними. За оцінками Forbes, до 2027 року ринкова вартість ШІ у сфері кібербезпеки досягне 46,3 мільярда доларів, оскільки все більше бізнес-лідерів користуються його можливостями для автоматизації даних, виявлення ризиків і захисту конфіденційної інформації.

Розуміння ландшафту кібербезпеки

Сучасний ландшафт кіберзагроз охоплює всі ризики, на які наражаються різні організації у відповідних контекстах. Кіберзагрози постійно еволюціонують у всі сфери діяльності, особливо з поширенням Інтернету та впровадженням цифрових технологій, що призводить до зростання цих ризиків. Численні інциденти в мережі залишаються постійною загрозою для всіх організацій, які працюють у віртуальному просторі.

За даними CNN, навіть уряд США залишається мішенню, ставши жертвою нещодавньої глобальної атаки, яка використала вразливість програмного забезпечення. Кілька сотень організацій по всій країні постраждали від цієї атаки. На кожен новий інструмент, який розробляється для захисту від кіберзлочинів, хакери створюють свій власний, і кількість випадків кіберзлочинів продовжує зростати.

За даними Північно-Західного університету, середня вартість витоку даних становить близько 4,27 мільйона доларів, тому організації повинні застосовувати надійні заходи кібербезпеки, щоб випереджати небезпеки. Застосування штучного інтелекту в кібербезпеці – це один з багатьох підходів до того, щоб залишатися гнучкими в динамічному просторі. Це інноваційний інструмент, який організації можуть використовувати для захисту конфіденційних даних і запобігання фінансовим і репутаційним наслідкам кібератак.

ШІ в кібербезпеці

Штучний інтелект – це широкий термін, що описує процес імітації людського інтелекту в машинах, щоб вони могли міркувати і використовувати логіку для вирішення проблем. Штучний інтелект у кібербезпеці базується на тому ж принципі: використання швидкості та обчислювальної потужності ШІ для створення протоколів кібербезпеки, які передбачають, ідентифікують та зменшують загрози.

На людські помилки припадає понад 80% кіберінцидентів і ШІ може заповнити цю прогалину, автоматизуючи завдання і розпізнаючи закономірності, невидимі для людського ока. Наприклад, алгоритми машинного навчання можуть класифікувати зловмисні атаки електронною поштою та виявляти схожі функції, які працівники можуть не помітити.

Такі інструменти, як обробка природної мови, можуть виявляти фішингову активність і шкідливе програмне забезпечення шляхом вилучення ключових слів.

Штучний інтелект навчається на власному досвіді. Генеративний ШІ перетинається з кібербезпекою, аналізуючи і навчаючись на величезних обсягах даних, щоб виявляти закономірності і приймати обґрунтовані рішення щодо реагування на потенційні загрози. Хоча він може вирішити лише деякі проблеми кібербезпеки, ШІ відіграє важливу роль у підтримці зусиль з кібербезпеки та дотриманні нормативних вимог.

Виявлення та запобігання загрозам

ШІ має значну перевагу над традиційними програмними системами у виявленні загроз. Оскільки він навчається на власному досвіді і працює швидше, ніж будь-яка людина, можна навчити його виявляти шкідливе програмне забезпечення, розпізнавати шаблони і помічати найнезначніші зміни.

Прогностичний інтелект –’ це ще одна сфера, у якій ШІ досягає успіху. Завдяки можливостям обробки природної мови штучний інтелект може переглядати статті в новинах, журналах і дослідженнях про кіберзагрози, створюючи чітку картину того, як вони можуть вплинути на вашу організацію.

Ось деякі з інших потенційних ризиків і обмежень:

Помилкові спрацьовування або негативи: ШІ може генерувати хибні спрацьовування – ідентифікуючи нешкідливі дії як зловмисні – і хибні негативи, роблячи протилежну помилку. Помилкові спрацьовування та негативи можуть бути складними для навігації, оскільки вони відволікають цінні ресурси на неіснуючі загрози або ігнорують наявні.

Етичні проблеми: хоча ШІ є революційним у сфері кібербезпеки, він створює етичні та регуляторні проблеми, особливо щодо конфіденційності даних. Наприклад, медичні організації повинні дотримуватися суворих правил HIPAA, щоб забезпечити конфіденційність інформації про пацієнтів.

Дефіцит навичок: ШІ є життєздатним варіантом лише для тих організацій, які мають доступ до кваліфікованих фахівців з кібербезпеки. Оскільки 63% організацій стверджують, що найбільший дефіцит навичок у них спостерігається у сфері ШІ та машинного навчання, подолання цього розриву може бути непростим завданням. Маючи необхідні навички та досвід, організації можуть усвідомити загальну цінність своїх інвестицій у ШІ та машинне навчання.

Якість даних. ШІ настільки ж ефективний, як і дані, на яких ви його тренуєте, і потребує великої кількості високоякісних даних, щоб підвищити точність. Багатьом організаціям важко отримати доступ до достатньої кількості цих високорівневих даних через проблеми конфіденційності та розмежованості.

Перевірка сайтів і безпека онлайн-транзакцій

Один із ключових аспектів захисту в цифровому просторі – це безпека вебсайтів, особливо тих, які використовують онлайн-транзакції. Для користувачів важливо перевіряти надійність сайтів перед тим, як здійснювати будь-які операції.

Як перевірити сайт на безпеку:

Шифрування SSL: переконайтеся, що сайт використовує захищений протокол SSL (https://). Це гарантує, що дані, які ви вводите, шифруються та захищаються під час передачі.

Перевірка домену: остерігайтеся підроблених сайтів, що імітують популярні платформи. Перевіряйте точність написання домену та сертифікати безпеки.

Огляди та рейтинги: перевіряйте відгуки про сайт, щоб переконатися у його надійності.

Користувачі, які взаємодіють із платформами, де здійснюються фінансові операції, повинні завжди перевіряти, чи захищені їхні дані. Онлайн-лотереї, як-от лото клуб онлайн, та інші сервіси можуть надавати чудові можливості для розваг, але важливо користуватися лише перевіреними платформами.

Висновки. Штучний інтелект вже зараз відіграє важливу роль у захисті від кіберзлочинів, але з кожною новою технологією виникають нові виклики. Зловмисники також вивчають можливості ШІ, що робить боротьбу з кіберзлочинністю постійною гонкою технологій. Для користувачів важливо не лише сподіватися на ШІ, але й бути обережними під час використання онлайн-платформ і перевіряти надійність сайтів перед здійсненням транзакцій.

Список використаних джерел:

1. https://cripo.com.ua/news/society/rol-shtuchnogo-intelektu-u-borotbi-z-kiberzlochynnistyu-chy-mozhut-tehnologiyi-vyperedyty-hakeriv/amp/
2. https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection