Давидов Петро.

Рев’ю публікації

«Використання Алгоритмів у бібліотеках мов програмування.»

Вступ

Публікація «Використання Алгоритмів у бібліотеках мов програмування» досліджує застосування алгоритмів і структур даних у кібербезпеці. Автори аналізують їхню роль у виявленні, запобіганні та пом'якшенні кіберзагроз, зосереджуючись як на класичних алгоритмах (шифрування, хешування), так і на сучасних технологіях, включаючи машинне навчання та квантову криптографію.

Основна мета: дослідження, виявлення ключових аспектів використання алгоритмів і структур даних для управління безпекою інформаційних систем.

Методологія

Дослідження спирається на огляд наукової літератури, а також на аналіз практичного застосування структур даних у системах безпеки. Автори розглядають алгоритми з позиції їхньої продуктивності, ефективності та стійкості до атак, використовують порівняльний аналіз різних методів, таких як криптографічні алгоритми, хеш-функції та графові структури. Також увага приділяється виявленню слабких місць алгоритмі, зокрема перед квантовими обчисленнями.

Результати

Основні результати дослідження включають:

- *Вплив алгоритмів на безпеку* - використання криптографії та хешування для захисту даних.
- *Важливість структур даних* - дерева, графи та хеш-таблиці забезпечують ефективне управління інформацією.
- *Роль AI та машинного навчання* - алгоритми аномального виявлення дозволяють та допомагають ідентифікувати загрози.
- *Загрози квантових обчислень* - розробка квантових та постквантових алгоритмів криптографії.

Ключові інсайти

Використання хеш-таблиць та графів.

Ці структури дозволяють зберігати та шукати сигнатури атак. Використання графів у моделюванні мережевих зв'язків підвищує якість аналізу загроз.

Застосування AI для виявлення аномалій.

Машинне навчання дозволяє аналізувати поведінку користувачів, виявляти певні «патерни», що неможливо зробити звичайними методами. Це відкриває нові можливості для «адаптивної» кібербезпеки. Що до, AI та його використання, то можливе, так зване: «використання «адаптивної» кібербезпеки».

Постквантова криптографія.

Квантові комп'ютери є конкурентами традиційним криптографічним алгоритмам, потрібна розробка нових сильних методів шифрування для безпеки цифрових систем.

Висновки

Публікація оглядає алгоритми і структури даних у кібербезпеці, підкреслюючи їхню критичну роль у забезпеченні цілісності, конфіденційності, доступності інформації. Головний посил роботи, це аналіз методів криптографії та моделей машинного навчання, що допомагає зрозуміти, як технологічний розвиток впливає на безпеку у технологіях.

Як варіант, у майбутньому, можна взяти до уваги оптимізацію AI-методів для боротьби з атакуючим машинним навчанням *(AML)* та впровадження криптографічних рішень у системи які використовуються.