активів; методи ансамблю для об'єднання прогнозів різних моделей та зменшення невизначеності. Приклади методів: ARIMA для аналізу часових рядів, баєсівські мережі для моделювання невизначеності у фінансових даних.

У роботі розглянуто актуальні аспекти використання статистичного навчання в умовах невизначеності та запропоновано практичні підходи до моделювання та управління невизначеністю у прогностичних моделях. Результати досліджень можуть бути використані для покращення точності та достовірності прогнозів у різних галузях застосування статистичного навчання. Підкреслено важливість розвитку адаптивних алгоритмів та використання баєсівського підходу для ефективного управління невизначеністю.

Список використаних джерел

1. Murphy, K. P. Machine Learning: A Probabilistic Perspective. MIT Press. 2021.

2. Машинне навчання. URL: https://uk.wikipedia.org/wiki/%D0% 9C%D0% B0%D1%88%D0%B8%D0%BD%D0%BD%D0%B5_%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BD%D0%BD%D1%8F (дата звернення: 02.12.2023).

3. Barber D. Bayesian reasoning and machine learning.Cambridge University Press. 2012.

УДК 004.056

Бондарєв О. О., Горін В. В., здобувачі вищої освіти 1 курсу спеціальності 125 Кібербезпека та захист інформації,

Ніколюк П. К., д-р фіз.-мат. наук, професор, професор кафедри інформаційних технологій

ЗВ'ЯЗОК МАТЕМАТИЧНОЇ КРИПТОГРАФІЇ ТА ОПТИМАЛЬНОГО КОДУВАННЯ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. Математична криптографія та оптимальне кодування є двома ключовими галузями інформаційних технологій, які спільно використовують математичні концепції для забезпечення безпеки й ефективності обміну інформацією. Ми розглянемо основні принципи цих двох галузей та їх взаємозв'язок. Математична криптографія є наукою, яка вивчає методи захисту інформації від несанкціонованого доступу. Основними завданнями криптографії є конфіденційність, цілісність та автентифікація інформації. Для досягнення цих цілей використовуються різні математичні алгоритми, як-от шифрування, підписи та інші методи [1].

Актуальність. Класифікація криптографічних алгоритмів (КА):

➢ Тайнопис. Відправник і одержувач роблять над повідомленням перетворення, відомі лише їм двом. Стороннім особам невідомий алгоритм шифрування. Деякі фахівці вважають, що тайнопис не є криптографією взагалі.

➢ КА з ключем. Алгоритм впливу на передані дані відомий усім стороннім особам, але він залежить від деякого параметра – «ключа», яким володіють лише відправник і одержувач.

➢ Симетричні КА. Для зашифровки і розшифровки повідомлення використовується один і той же блок інформації (ключ).

➢ Асиметричні КА. Це такий алгоритм, який для зашифровки повідомлення використовує один («відкритий») ключ, відомий усім охочим, а для розшифровки – інший («закритий») ключ, який існує тільки в одержувача.

Залежно від кількості ключів, які застосовуються у конкретному алгоритмі:

➢ Безключові КА – не використовують в обчисленнях жодних ключів.

➢ Одноключові КА – працюють з одним додатковим ключовим параметром (якимсь таємним ключем).

➢ Двоключові КА – на різних стадіях роботи в них застосовуються два ключові параметри: секретний та відкритий ключі.

Залежно від характеру впливів, що виробляються над даними, алгоритми підрозділяються на:

➢ Перестановочні – блоки інформації (байти, біти, більші одиниці) не змінюються самі по собі, але змінюється їх порядок проходження, що робить інформацію недоступною сторонньому спостерігачеві.

➢ Підстановочні – самі блоки інформації змінюються за законами криптоалгоритму. Переважна більшість сучасних алгоритмів належить цій групі.

Залежно від розміру блоку інформації криптоалгоритми поділяються на:

➢ Потокові шифри – одиницею кодування є один біт. Результат кодування не залежить від попереднього вхідного потоку. Схема застосовується в системах передачі потоків інформації, тобто в тих випадках, коли передача інформації починається і закінчується в довільні моменти часу і може випадково перериватися. Найбільш поширеними представниками потокових шифрів є скремблери.

➢ Блочні шифри – одиницею кодування є блок із декількох байтів (діапазон кодування знаходиться в межах 4–32 байтів).

Результат кодування залежить від усіх вихідних байтів цього блоку. Схема, що застосовується під час пакетної передачі інформації та кодування файлів, представлена на рис. 1 [2].

Алгоритми шифрування базуються на математичних операціях, які ускладнюють процес розшифрування без наявності відповідного ключа. Криптографічні протоколи, як-от RSA, ECC та інші, використовують абстракції алгебричних

структур, як-от групи та поля. Оптимальне кодування є галуззю теорії інформації, яка займається розробкою кодів для передачі та збереження інформації з мінімальною кількістю біт. Це означає, що коди мають ефективно використовувати ресурси та забезпечувати найменший можливий обсяг інформації. Основним поняттям в оптимальному кодуванні є ентропія, яка визначає середню кількість біт, необхідних для кодування символа [3]. Коди, які наближаються до цієї ентропії, вважаються оптимальними. Обидві галузі використовують математичні концепції для досягнення своїх цілей. У криптографії використовуються алгебричні структури для створення надійних систем шифрування та підпису. Водночас оптимальне кодування використовує теорію інформації та ймовірності для створення ефективних кодів. Одним із прикладів взаємодії цих галузей є застосування кодів для захисту переданих криптографічно зашифрованих повідомлень. Використання оптимальних кодів дає змогу ефективно передавати інформацію за мінімальних витрат ресурсів. Математична криптографія та оптимальне кодування є ключовими галузями, що забезпечують безпеку й ефективність обміну інформацією в інформаційному суспільстві. Їх взаємозв'язок виявляється у використанні спільних математичних концепцій для досягнення відповідних цілей, створюючи у такий спосіб основу для розвитку сучасних технологій безпеки та збереження інформації [4].

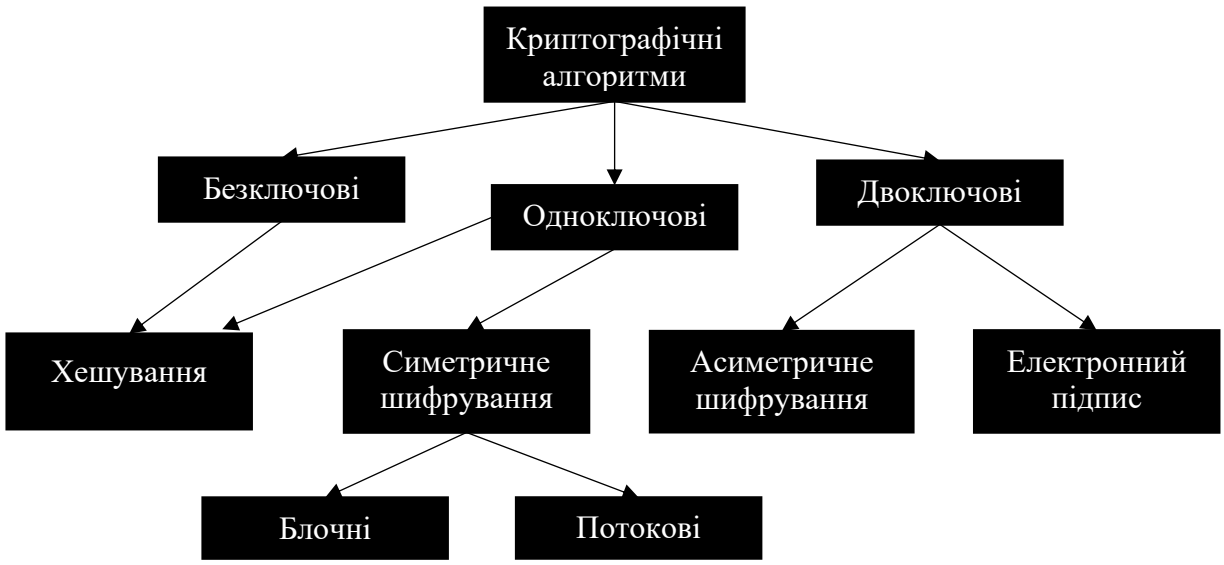

Рисунок 1. Структура криптографічних алгоритмів

Висновки. Обидві галузі спільно сприяють забезпеченню ефективної та безпечної передачі інформації, застосовуючи математичні концепції й алгоритми. Математична криптографія забезпечує захист, використовуючи складні математичні методи, тоді як оптимальне кодування максимізує ефективність використання ресурсів для ефективної обробки та передачі даних.

Список використаних джерел

1. Математичні основи криптографії: URL: https://cutt.ly/SwYzQnGY (дата звернення: 13.11.2023).
2. Wikipedia. URL: https://cutt.ly/IwYzQ2mz (дата звернення: 13.11.2023).
3. Оптимальне кодування. URL: https://cutt.ly/gwYzWSOm (дата звернення: 13.11.2023).
4. Математична криптографія та оптимальне кодування. URL: https://cutt.ly/gwqzMSDa (дата звернення: 13.11.2023).

УДК 004.8

Бурківський О. С., здобувач 2 курсу спеціальності 122 Комп'ютерні науки,
Зелінська О. В., канд. техн. наук, доцент, в. о. завідувача кафедри інформаційних технологій

СУЧАСНІ ФРЕЙМВОРКИ МАШИННОГО НАВЧАННЯ

Донецький національний університет імені Василя Стуса, м. Вінниця

Сучасний розвиток технологій у галузі машинного навчання визначається більшою мірою використанням потужних фреймворків. Ці інструменти не лише прискорюють розробку моделей, а й надають розробникам та дослідникам гнучкість і можливості для ефективного впровадження інтелектуальних систем. У публікації ми розглянемо кілька ключових сучасних фреймворків машинного навчання.

TensorFlow є високопродуктивним відкритим вихідним фреймворком для машинного та глибокого навчання, розробленим і підтримуваним Google. Запущений у 2015 р., він завоював широку популярність завдяки своїй гнучкості, ефективності та розширеною підтримкою глибокого навчання.

Особливості TensorFlow:

1. TensorFlow дає змогу розробникам вибирати між статичною та динамічною обчислювальною графікою. Це забезпечує гнучкість під час вибору оптимального підходу до розробки моделей.

2. Вона також має великий набір заздалегідь вбудованих шарів для різних видів мереж, а також оптимізаторів для тренування моделей із різною складністю.

3. Підтримка роботи на різноманітних апаратних платформах дає змогу ефективно використовувати ресурси для тренування великих моделей.

4. TensorFlow має активну та велику спільноту користувачів та розробників. Це забезпечує доступ до різноманітних ресурсів, зокрема документації, навчальних матеріалів та багатофункціональних модулів.