

```

if (signature.R < 1 || signature.R > curve.N - 1)
{
    return false;
}

if (signature.S < 1 || signature.S > curve.N - 1)
{
    return false;
}

var w = MathHelper.Inv(signature.S, curve.N);
var u1 = (numberMessage * w) % curve.N;
var u2 = (signature.R * w) % curve.N;
var point = MathHelper.Add(MathHelper.Multiply(curve.G, u1, curve.N, curve.A, curve.P),
MathHelper.Multiply(this.Point, u2, curve.N, curve.A, curve.P), curve.A, curve.P);

if (point.X == 0 && point.Y == 0)
{
    return false;
}

return point.X % curve.N == signature.R;
}
}

```

Отже, ECDSA забезпечує високу криптографічну безпеку для блокчейн-транзакцій, використовуючи еліптичні криві. Реалізація класів PrivateKey і PublicKey на C# дає змогу ефективно підписувати та перевіряти повідомлення, що є основою для безпеки у блокчейн-мережах.

Список використаних джерел

1. Elliptic Curve Digital Signature Algorithm. *HYPR*. URL: <https://surl.li/lxxejp> (дата звернення: 20.12.2024).
2. Raza S. Ethereum's Elliptic Curve Digital Signature Algorithm (ECDSA). *Medium*. 2023. URL: <https://fitsaleem.medium.com/ethereums-elliptic-curve-digital-signature-algorithm-ecdsa-88e1659f4879>

УДК 004.415.28

*Перепелиця А. С., здобувач вищої освіти,
Бабаков Р. М., д-р техн. наук, професор
кафедри інформаційних технологій*

ІНФОРМАЦІЙНА ПЛАТФОРМА ДЛЯ АНАЛІЗУ НАВЧАННЯ ТА КАР'ЄРНИХ МОЖЛИВОСТЕЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Проблема вибору майбутньої професійної траєкторії є актуальною для старшокласників, які часто стикаються з невизначеністю, зумовленою недостатньою поінформованістю про їхні здібності, інтереси та можливості на ринку праці [1, 2]. Для розв'язання цієї проблеми було розроблено інформаційну

систему, яка узагальнює результати навчання учнів і надає персоналізовані рекомендації щодо вибору спеціальності для вступу в університет.

Сучасна освіта активно інтегрує інформаційні технології [3], які дають змогу автоматизувати аналіз даних і підтримувати прийняття рішень. Унікальність запропонованої системи полягає у поєднанні функцій журналювання академічних досягнень із базовою профорієнтацією, заснованою на результатах психометричного аналізу. Це сприяє більш усвідомленому вибору професійного шляху, забезпечує комплексний аналіз особистості та уникає суб'єктивності у профорієнтаційних рекомендаціях, яка може виникнути через людський фактор.

Основні завдання такої платформи [4]:

- 1) Розробити інструментарій для збору та обробки навчальних даних і психометричного тестування.
- 2) Інтегрувати моделі штучного інтелекту для формування персоналізованих рекомендацій.
- 3) Забезпечити доступ до системи для учнів, вчителів і батьків із різними рівнями прав доступу.
- 4) Реалізувати функції звітування, які допоможуть надавати рекомендації у зручному форматі.

Розроблена платформа базується на таких технологіях:

- Бекенд реалізований на Kotlin із використанням фреймворка Spring Boot. Spring Boot є потужним і функціональним фреймворком, що забезпечує стабільність роботи системи, а модуль Spring Security забезпечує механізми автентифікації, авторизації та захисту від атак, як-от CSRF, SQL-ін'єкції тощо.
- Фронтенд створено за допомогою JavaScript і бібліотеки React, що гарантує адаптивність і зручність користувацького інтерфейсу.
- Для зберігання даних використано об'єктно-реляційну СУБД PostgreSQL, яка відповідає вимогам до масштабованості й обробки великих обсягів даних.
- Модель штучного інтелекту, що використовується для профорієнтаційних рекомендацій, реалізована із застосуванням платформи H2O.ai. Це дає змогу аналізувати навчальні досягнення у поєднанні з результатами психологічного тестування та, за потреби, надає можливість модифікувати модель ШІ, аби надалі за наявності більшої кількості даних давати більш точні передбачення, базуючись на реальних кейсах вступу випускників.

Наразі на платформі реалізовано такий функціонал:

- 1) Централізоване збереження даних про успішність учнів і результати психометричних тестів.
- 2) Генерація профорієнтаційних рекомендацій на основі аналізу даних. Зокрема, враховується весь перелік навчальних предметів, затверджений Міністерством освіти і науки України, і на платформі є можливість пройти психологічні тести для психометричного аналізу. Наразі для проходження доступні тести Айзенка та Голланда [5].
- 3) Кросплатформений доступ до інформації для учнів, вчителів і батьків через багаторівневу систему авторизації.

4) Система видів роботи, що дає можливість у межах одного уроку оцінити роботу учня за різними видами активностей, не переносячи оцінки на клітинки інших днів (як це виглядає для вчителя, показано на рис. 1).

11-Б											
Вересень	Жовтень	Листопад	Грудень	Січень	Лютий	Березень	Квітень	Травень	Червень	Листопад	Грудень
Дата	06.10	07.10	08.10								
Номер уроку	1	1	1								
Атаманенко Софія											
Башко Денис		6/12									
Бегей Аліна			8/24								
Білінський Олексій											
Бурбан Василина		10/12			9/12						
Візний Ігор				11/12			5/12				

Рисунок 1 – Інтерфейс редагування кількох оцінок у межах одного уроку

Розроблена система допомагає:

- 1) знизити рівень стресу та невизначеності серед учнів під час вибору професійної траєкторії;
- 2) надати учням обґрунтовані рекомендації, які сприятимуть їхньому професійному та особистісному розвитку;
- 3) забезпечити вчителям і батькам зручні інструменти для моніторингу навчального прогресу й підтримки учнів у їхніх рішеннях.

Інформаційна система для аналізу навчання та кар'єрних можливостей є інноваційним рішенням, що об'єднує автоматизацію освітнього процесу з проф-орієнтаційною підтримкою. Її впровадження дасть змогу підвищити якість освітнього процесу, сприяти усвідомленому вибору професії та поліпшити підготовку учнів до викликів ринку праці.

Список використаних джерел

1. Sihite J. The student preference to choose higher education: a case study in west Jakarta 2019. *European journal of business and mangement*. 2019. № 25. С. 59–64. URL: <https://core.ac.uk/download/pdf/276531308.pdf> (дата звернення: 20.12.2024).
2. Шкіль Л. Тільки кожен шостий студент закінчує ІТ-курси до кінця – дослідження. *AIN.UA*. URL: <https://ain.ua/2023/01/05/tilky-kozhen-shostyj-student-zakinchuye-it-kursy-do-kinczya-doslidzhennya/> (дата звернення: 20.12.2024).
3. Електронні класні журнали та щоденники з можливостями дистанційного навчання. *Нові Знання*. URL: <https://nz.ua> (дата звернення: 20.12.2024).
4. Перепелиця А. С., Бабаков Р. М. Інформаційна система для узагальнення результатів навчання з функцією проф-орієнтації. *Прикладні аспекти сучасних міждисциплінарних досліджень*: Всеукр. науково-практ. конф., (м. Вінниця, 1 листоп. 2024 р.). Вінниця, 2024. URL: <https://jpasmd.donnu.edu.ua> (дата звернення: 20.12.2024).

5. Опитувальник професійної спрямованості (ОПС) Д. Голанда. *Тернопільський обласний центр зайнятості*. URL: <https://ter.dcz.gov.ua/publikaciya/opytuvalnyk-profesiynoyi-spryamovanosti-ops-d-golanda> (дата звернення: 20.12.2024).

УДК 004.056:004.052;004.652

*Плець В. В., здобувач вищої освіти,
Потапова Н. А., канд. екон. наук., доцент,
доцент кафедри інформаційних технологій*

ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЙ І ХЕШ-ТАБЛИЦЬ У КІБЕРБЕЗПЕЦІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Хеш-функція – це математичний алгоритм, який перетворює дані довільної довжини (текст, числа, файли тощо) у хеш-значення (також відоме як хеш або дайджест) фіксованого розміру. Незалежно від розміру вхідних даних, результатом роботи хеш-функції завжди буде рядок однакової довжини, що робить її корисною для багатьох завдань, як-от:

1. Перевірка цілісності даних: хешування використовується для створення контрольних сум, які дають змогу перевіряти, чи не було змінено дані під час передачі або зберігання.

2. Захист паролів: у базах даних замість збереження паролів зберігають їх хеші, що підвищує безпеку.

3. Цифрові підписи та сертифікати: хеш-функції використовуються в криптографії для створення підписів і перевірки автентичності даних.

4. Оптимізація пошуку: у структурах даних, як-от хеш-таблиці, хешування допомагає швидко знаходити потрібні елементи.

Хороша хеш-функція повинна відповідати таким властивостям: детермінованість (однакові вхідні дані завжди дають один і той самий хеш), швидкість (обчислення хешу має бути ефективним), стійкість до колізій (різні вхідні дані повинні давати різні хеш-значення), невідворотність (за хеш-значенням має бути практично неможливо відновити початкові дані).

Популярні хеш-функції включають MD5, SHA-1, SHA-256 та інші. Однак деякі старі функції, як-от MD5 і SHA-1, більше не вважаються безпечними через вразливість до колізій [1]. На рис. 1 та 2 наведено обчислення хешу на C# (SHA-256) та результат виконання програмного коду.

Хеш-таблиці та хеш-функції відіграють ключову роль у сучасних системах кібербезпеки завдяки своїй здатності ефективно обробляти великі обсяги даних та забезпечувати захист від несанкціонованого доступу. Хеш-функції використовуються для створення унікальних і незворотних значень, що допомагають забезпечити цілісність і автентичність даних, а також створюють основи для алгоритмів підпису та перевірки повідомлень. Натомість хеш-таблиці є важливим інструментом для швидкого пошуку та перевірки великих наборів даних, як-от списки заблокованих IP-адрес чи паролів, що підвищує ефективність кіберзахисту.