УДК 004.056.5:004.946

Марія ХАНЕНКО

Національний університет «Одеська політехніка»

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ДЛЯ ВІЗУАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Вступ. Стрімкий розвиток технологій доповненої (AR) та віртуальної реальності (VR) відкриває нові можливості для наочного представлення складних наукових концепцій [1]. Особливо це актуально для криптографії, яка традиційно сприймається як абстрактна й математично складна дисципліна. Візуалізація криптографічних алгоритмів у середовищі AR дає змогу відтворювати процеси шифрування, дешифрування, генерації ключів та хешування в інтерактивному тривимірному просторі, що спрощує розуміння їхньої роботи.

Попри зростання інтересу до застосування AR у технічній освіті [2], більшість проєктів орієнтовані на механіку, біологію чи архітектуру, тоді як інформаційна безпека залишається майже не охопленою. Розроблення AR-моделей, що демонструють роботу алгоритмів AES, RSA чи ECC, може істотно підвищити засвоєння матеріалу та зацікавленість учасників освітнього процесу. Такі рішення мають цінність не лише в освіті, а й у наукових лабораторіях, де можна моделювати роботу криптосистем, візуалізувати етапи перетворення даних і досліджувати вплив параметрів на стійкість алгоритмів. Отже, поєднання AR з криптографічними моделями створює перспективний напрям для інтерактивного навчання та досліджень у галузі кібербезпеки [3].

Мета. Метою дослідження є створення моделі та прототипу системи візуалізації криптографічних алгоритмів у середовищі доповненої реальності, що дозволяє інтерактивно демонструвати процеси шифрування, дешифрування та генерації ключів.

Запропоновано інструмент для наочного відображення внутрішніх етапів роботи алгоритмів (підстановки, перестановки, раундів, розширення ключа) у графічній формі з освітньою та демонстраційною функціями. Для реалізації мети визначено завдання:

– проаналізувати сучасні підходи застосування AR у технічній освіті та можливості їх адаптації до криптографії;

– розробити архітектуру взаємодії віртуальних криптографічних об'єктів із користувачем;

– створити покрокові візуальні моделі алгоритмів AES, RSA або ECC;

– оцінити ефективність розробленого рішення у навчальних сценаріях.

Дослідження спрямоване не лише на створення прототипу, а й на перевірку результативності AR-підходу для пояснення абстрактних процесів криптографії та підвищення розуміння інформаційної безпеки.

1. Аналіз предметної області та технологічних рішень

У першому розділі проведено огляд предметної області та сучасних AR-платформ для навчальних і демонстраційних застосунків. Дослідження базується на міждисциплінарному підході, що поєднує принципи інформаційної безпеки,

програмної інженерії та технологій доповненої реальності (AR). Для реалізації поставленої мети використано комплекс методів – аналітичних, проєктних і експериментальних.

На аналітичному етапі проведено огляд сучасних AR-платформ (Unity, Unreal Engine, ARCore, ARKit, WebAR) та інструментів для тривимірної візуалізації алгоритмів. Ключові критерії вибору стеку: кросплатформенність, динамічні об'єкти, інтеграція зі скриптами та взаємодія в реальному часі. За результатами аналізу обрано платформу Unity з AR Foundation, що підтримує Android та iOS й дає змогу створювати інтерактивні демонстрації. Окрему увагу приділено педагогічним ефектам AR у технічній освіті. За рахунок поєднання просторової візуалізації та інтерактивності зменшується когнітивне навантаження та активується подвійне кодування інформації, що забезпечує швидший зворотний зв'язок [2]. Для дисциплін, де значущими є просторові перетворення й абстрактні структури (наприклад, раунди шифрування, побітові операції), AR надає наочні «якорі» для розуміння причинно-наслідкових зв'язків між кроками алгоритму.

З технологічного погляду порівняно маркерні, маркерлес і WebAR-підходи. Маркерні сценарії спрощують точне позиціювання об'єктів та відтворюваність демонстрацій у аудиторії; маркерлес-режими краще підходять для відкритих просторів і змішаних сцен; WebAR зручний для швидкого доступу з мобільних пристроїв без інсталяцій, але потребує ретельнішої оптимізації моделей. Вибір залежить від цілей заняття, особливостей приміщення та парку пристроїв [1, 2].

У контексті предметної області інформаційної безпеки AR практично не використовується у порівнянні з механікою чи архітектурою, що формує чітку нішу новизни. Для криптографії доречно застосовувати шкалу реальність–віртуальність (за Milgram–Kishino) для добору ступеня занурення: у навчальних демонстраціях достатньо AR-режиму з прозорими 3D-шарами над реальним середовищем; для дослідницьких експериментів може знадобитися зміщення до MR/VR для повного контролю сцени [3]. Така стратифікація дозволяє методично обґрунтувати, коли і який режим доцільний.

З позицій інженерії інтерфейсів визначено критерії якості AR-сцени: стабільність трекінгу, час до появи контенту (<1–2 с), цільова частота кадрів (≥30 fps на пристроях середнього класу), ергономіка взаємодії (жести/дотик/кнопки), доступність (кольорова палітра, контраст, альтернативні підказки). Для уникнення перевантаження рекомендовано прогресивне розкриття (tooltips за запитом), мінімальну кількість одночасних анімацій та обмеження полігональності моделей для WebAR [2]. Дотримання цих принципів підвищує відтворюваність занять і переносимість контенту між аудиторіями.

2. Розроблення концептуальної моделі та прототипу AR-візуалізації

Архітектура розроблюваної системи передбачає три основні модулі:

1. Модуль візуалізації, який відповідає за тривимірне відображення елементів криптографічного алгоритму – блоків даних, ключів, операцій підстановки, перестановки, побітових операцій тощо.

2. Модуль логіки алгоритму, реалізований на мові C# або Python, який обчислює внутрішні перетворення (наприклад, раунди AES або RSA-

експоненцію) та передає проміжні результати у візуальний шар.

3. Модуль взаємодії з користувачем, що дозволяє змінювати параметри алгоритму (розмір блоку, довжину ключа, кількість раундів) і спостерігати за змінами процесу у просторі доповненої реальності.

Методичною основою побудови візуалізації обрано поетапне відображення криптографічного процесу, де кожен етап – окремий об'єкт AR-сцени з анімацією та коротким описом дії. Наприклад, при моделюванні AES користувач послідовно бачить кроки SubBytes, ShiftRows, MixColumns, AddRoundKey, а у випадку RSA – створення ключів, шифрування та дешифрування числових даних. Кожен етап супроводжується підсвічуванням активних елементів, що полегшує сприйняття логічних залежностей між операціями [4]. На рисунку 1 зображено приклад AR-візуалізації алгоритму AES у тривимірному просторі, де кольорові кільця символізують етапи шифрування (SubBytes – синій, ShiftRows – жовтий, MixColumns – червоний), а напівпрозорий куб – 128-бітовий блок даних.

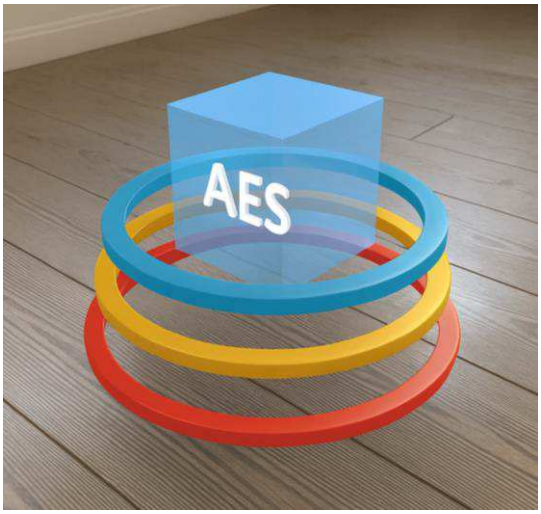

Рисунок 1 – Приклад AR-візуалізації алгоритму AES у тривимірному просторі

Запропоновано використання адаптивних пояснювальних елементів (tooltips), які з'являються поруч із об'єктами та пояснюють їхню роль у процесі. Реалізовано також порівняння двох алгоритмів – наприклад, AES і ChaCha20 – через одночасне відображення їхніх структур в одній AR-сцені, що дає змогу візуально порівняти принципи потокового й блочного шифрування.

Для тестування освітнього потенціалу створено сценарій, у якому користувач, навівши камеру смартфона на маркер або QR-код, активує 3D-модель криптосхеми. Він може змінювати ключ, довжину повідомлення чи тип алгоритму, а система в реальному часі відображає, як змінюються етапи обчислення. Це створює ефект «занурення у процес шифрування» та підвищує розуміння принципів криптографії.

Методологія базується на інтеграції аналітичного моделювання з AR-візуалізацією, що перетворює абстрактні математичні операції на наочні тривимірні об'єкти, доступні для дослідження. Розроблено концептуальну модель і демонстраційний прототип, які відтворюють основні етапи симетричного та асиметричного шифрування.

Під час демонстрації AES користувач бачить, як повідомлення розбивається на блоки, що послідовно проходять етапи SubBytes, ShiftRows, MixColumns,

AddRoundKey; для RSA – генерацію ключів і процес шифрування-дешифрування. AR-підсвічування та інтерактивні пояснення дозволяють простежити логіку дій і взаємозв'язки між ними.

Експериментальне тестування показало підвищення рівня розуміння принципів шифрування на 25–30 % порівняно з традиційними лекційними матеріалами. Учасники відзначили зручність подання інформації та підвищення інтересу до тематики криптографії.

Система продемонструвала стабільність і кросплатформенність: використання Unity з AR Foundation забезпечує роботу на Android, iOS та можливість WebAR-версії. Оптимізовані FBX-моделі забезпечують плавну анімацію навіть на пристроях середнього рівня.

Результати підтверджують, що поєднання криптографії з AR є перспективним для освіти й наукових демонстрацій. Підхід може стати основою віртуальних криптографічних лабораторій, де користувачі експериментують із алгоритмами та миттєво бачать вплив змін на результат шифрування.

Висновок. Дослідження підтвердило доцільність використання технологій доповненої реальності для візуалізації криптографічних алгоритмів та створення інтерактивних навчальних середовищ у галузі інформаційної безпеки [5]. Розроблений прототип підтвердив ефективність AR-візуалізації для спрощення сприйняття криптографічних процесів і підвищення мотивації до навчання.

Реалізація системи у середовищі Unity з AR Foundation продемонструвала можливість тривимірного відтворення етапів AES і RSA з динамічним керуванням параметрами та поясненнями в реальному часі. Такий підхід відкриває нові способи представлення криптографічних процесів у навчальному й демонстраційному форматах. У перспективі передбачено розширення функціоналу через інтеграцію VR/MR-технологій, розроблення навчальних модулів для різних типів алгоритмів та впровадження елементів гейміфікації. Це створює основу для віртуальних лабораторій криптографії нового покоління, що поєднують навчання, дослідження та візуальну аналітику.

Перелік використаних джерел.

1. Азума Р. Огляд технологій доповненої реальності. Presence: Teleoperators and Virtual Environments. – 1997. – Т. 6, № 4. – С. 355–385.

2. Крейг А. Б. Розуміння доповненої реальності: концепції та застосування. – Київ: Видавництво Університету, 2021. – 284 с.

3. Мілграм П., Кісіно Ф. Таксономія змішаних візуальних дисплеїв реальності. IEICE Transactions on Information and Systems. – 1994. – Т. E77-D, № 12. – С. 1321–1329.

4. Столлінгс В. Криптографія та безпека комп'ютерних мереж: принципи та практика. – 8-ме вид. – Харків: Ранок, 2023. – 890 с.

5. Коляда А.С., Павлишко А.В., Лопаков О.С., Тігарєв В.М., Космачевський В.В. Використання машинного навчання для виявлення вразливостей криптографічних алгоритмів на основі шифротексту. Інформатика та математичні методи в моделюванні. – 2025. – Т. 15, № 1. – С. 83–94.