Hryniaieva // CEUR Workshop Proceedings : 11th Workshop on Cloud Technologies in Education, CTE 2023 (22 December 2023). – Kryvyi Rih, 2024. – Vol 3679. – P. 54-66.
2. Гевко І. В.Формування і розвиток професіоналізму вчителя технологій: теорія і методика: монографія. Кам'янець-Подільський: Аксіома, 2017. 392 с.
3. Ожга М. М. Формування графічних компетентностей в майбутніх фахівців професійно-технічної освіти / М. М. Ожга, Х. В. Новіцька // Актуальні проблеми та перспективи технологічної і професійної освіти : матеріали VI-ї Всеукраїнської науково-практичної інтернет-конференції (м. Тернопіль, 24-25 травня 2021 р.). – Тернопіль : ТНПУ ім. В. Гнатюка, 2021. – С.50-51.
4. Про комп'ютерну графіку як інструмент навчання і професійної діяльності вчителя. В.Г. Шамоня, О.М. Удовиченко, А.О. Юрченко. Наукові доповіді викладачів фізико-математичного факультету. Суми: Вид-во фізико-математичного факультету СумДПУ імені А.С. Макаренка, 2017. Випуск 2. С.48-52.

Пендаківський Зеновій
Науковий керівник – доц. Ящик Олександр

МЕТОДИЧНІ ПІДХОДИ ДО ВИКЛАДАННЯ КРИПТОГРАФІЇ

Методичні підходи до викладання криптографії зазвичай базуються на поєднанні теоретичних основ та практичного застосування. Ця дисципліна охоплює як математичні концепції, так і комп'ютерну реалізацію алгоритмів, тому ефективне навчання вимагає інтегрованого підходу. Перш за все, викладання починається з формування фундаментального розуміння базових понять: інформаційна безпека, шифрування, криптоаналіз, симетричні й асиметричні алгоритми, хеш-функції. Це забезпечує міцну теоретичну базу, на якій потім будується розгляд більш складних тем. Важливо пояснювати не лише як працює той чи інший метод, але й навіщо він потрібен, в яких ситуаціях застосовується, які має обмеження. Вподальшому доцільно впроваджувати практичні завдання, що дасть змогу студентам власноруч реалізовувати криптографічні алгоритми – наприклад, реалізацію RSA або AES у програмному коді. Це не лише закріплює знання, а й сприяє розвитку навичок програмування та аналітичного мислення.

Одним із важливих підходів є використання історичних прикладів та реальних кейсів. Наприклад, розгляд шифру Цезаря чи Енігми дає змогу краще зрозуміти еволюцію криптографії, а аналіз сучасних атак – актуалізує знання. Також важливу роль відіграє міждисциплінарність. Криптографія перетинається з математикою (особливо з теорією чисел, алгеброю), інформатикою (структури даних, алгоритми, програмування), правом (регулювання захисту даних) та навіть філософією (питання приватності й етики в цифровому просторі). Це дозволяє подати матеріал у ширшому контексті. Також, сучасні підходи до викладання криптографії часто передбачають інтерактивні засоби навчання: онлайн-платформи, симулятори криптографічних протоколів, участь у CTF-змаганнях (Capture The Flag), де студенти можуть застосувати знання на практиці, змагаючись у розв'язанні завдань з інформаційної безпеки. Таким чином, методика викладання криптографії має бути різноплановою, включати як глибоке вивчення теорії, так і активну практичну діяльність, спрямовану на закріплення знань та розвиток професійних компетенцій.

Поєднання теоретичних основ та практичного застосування у викладанні криптографії – це не просто чергування лекцій і лабораторних занять, а цілісний підхід, який дозволяє зробити знання "живими", гнучкими і адаптивними до сучасних викликів у сфері безпеки. Теорія дає розуміння структури й принципів, але лише практика показує, як ці принципи працюють у конкретних ситуаціях. Наприклад, розглядаючи алгоритм RSA, студент спочатку вивчає математичну базу – модульну арифметику, теорему Ейлера, прості числа – а вже потім власноруч реалізовує генерацію ключів, шифрування та розшифрування, стикаючись із проблемами на кшталт вибору довжини ключа, ефективності обчислень чи обробки помилок. У такий спосіб знання перетворюються з абстрактних формул у робочі інструменти.

Крім того, така інтеграція дозволяє побачити різницю між "ідеальною" математичною моделлю і її реалізацією у програмному середовищі. Наприклад, на рівні формул цифровий підпис – це просте перетворення, але коли студенти працюють із бібліотеками типу OpenSSL або PyCryptodome, вони зіштовхуються з такими речами, як кодування повідомлень, керування ключами, перевірка підпису в різних форматах. Це стимулює не лише глибше розуміння самого алгоритму, а й розвиток аналітичного мислення, вміння враховувати деталі та перевіряти безпеку на всіх етапах.

Також варто згадати про зворотній зв'язок між теорією і практикою: іноді саме через практичні завдання студенти починають ставити глибші запитання про теоретичні аспекти. Наприклад, чому не можна використовувати один і той самий ключ у симетричному шифруванні для тривалого зберігання інформації? Або чому деякі хеш-функції більше не вважаються безпечними, хоча математично вони виглядають доволі стійко? Такі запитання дають змогу розширити теоретичну базу, перейти від поверхневого запам'ятовування до критичного осмислення. У підсумку, викладання криптографії, побудоване на гармонійному поєднанні теорії та практики, формує у студентів не лише знання, а й здатність використовувати їх в реальних умовах – саме це й відрізняє спеціаліста від просто "знаючої людини".

Формування фундаментального розуміння базових понять криптографії починається з усвідомлення її цілі – захисту інформації в умовах, коли вона передається чи зберігається в потенційно небезпечному середовищі. Студент має відчути, що криптографія – це не просто набір технічних прийомів, а відповідь на дуже конкретну потребу: забезпечити конфіденційність, цілісність, автентичність та доступність даних. Зрозумівши це, він починає сприймати всі подальші терміни – шифрування, ключ, цифровий підпис – як частини єдиного механізму, а не окремі складові, які потрібно просто вивчити.

Однією з перших речей, яку потрібно закласти – це інтуїція щодо того, як працює шифрування: є повідомлення, є правило (алгоритм), за допомогою якого повідомлення перетворюється у щось незрозуміле, і є ключ, без якого неможливо повернутися до оригіналу. Це базове уявлення – про співвідношення відкритого тексту, зашифрованого тексту та ключа – лежить в основі майже всіх подальших тем. Окрему увагу варто приділяти розрізненню між

симетричним і асиметричним шифруванням. Тут важливо не просто запам'ятати, що в першому випадку ключ один, а в другому – два, а зрозуміти, які саме проблеми вирішує кожен з підходів. Наприклад, питання безпечної передачі ключа у симетричній схемі приводить до появи ідеї публічного ключа – і так студенти природно приходять до теми асиметричних алгоритмів. Таким чином, знання формується не як перелік фактів, а як логічно збудована система.

Формуючи фундамент, викладач має також поступово знайомити студентів із загрозами – хто і навіщо може намагатися зламати систему, які типи атак існують, чому недостатньо просто «сховати» інформацію. Це відкриває перед студентами криптографію не як абстрактну науку, а як живу сферу, що розвивається у відповідь на реальні загрози. Саме в такому контексті формуються ідеї криптостійкості, довжини ключів, стійких хеш-функцій. Коли студент розуміє, що кожен елемент системи – це частина оборони, яка має витримати конкретні типи атак, він починає сприймати криптографію не лише як набір технік, а як систему захисту з власною логікою й архітектурою. Таким чином, фундаментальне розуміння криптографії не обмежується знанням термінів – воно включає здатність бачити загальну картину: чому певні речі працюють саме так, як вони працюють, і яку роль вони відіграють у ширшому контексті захисту інформації.

Практичні завдання у викладанні криптографії відіграють надзвичайно важливу роль, оскільки дозволяють студентам перейти від теоретичного розуміння до реального застосування знань. Вони створюють той міст між абстрактними формулами та конкретними сценаріями, в яких захист інформації набуває критичного значення. Ці завдання зазвичай розробляються таким чином, щоб поступово ускладнюватися: від простих реалізацій базових шифрів до складних проєктів, що моделюють сучасні протоколи захисту.

На початкових етапах студентам пропонують власноруч реалізувати класичні шифри на кшталт шифру Цезаря, Віженера або одноразового блокнота. Це дає змогу глибше зрозуміти принципи шифрування та дешифрування, а також побачити на практиці, наскільки легко або важко зламати той чи інший метод без знання ключа. Такий досвід формує інтуїцію щодо важливості криптостійкості й довжини ключа. Поступово завдання переходять до реалізації сучасних алгоритмів – наприклад, симетричних (AES) або асиметричних (RSA, ElGamal). Тут студенти вже не просто пишуть код, а стикаються з питаннями ефективності, генерації ключів, форматування даних для шифрування, правильного вибору режиму (наприклад, ECB vs. CBC для AES). У процесі вони вчаться працювати з бібліотеками, писати безпечний код, розуміти специфіку реалізації криптографії в реальних мовах програмування. Особливе місце займають завдання, що стосуються хеш-функцій та цифрового підпису. Студенти не просто створюють хеш від повідомлення, а, наприклад, перевіряють цілісність файлу після передачі, експериментують з колізіями, або навіть проводять примітивний аналіз вразливостей у слабших алгоритмах типу MD5. У цифровому підписі особливу увагу приділяють перевірці автентичності та створенню повноцінних схем підпису та перевірки з відкритим ключем.

Ближче до завершення курсу студенти виконують завдання, які моделюють реальні криптографічні протоколи. Наприклад, обмін ключами за схемою Діффі-Геллмана або побудову мініатюрної TLS-сесії. Тут уже необхідно враховувати багато факторів: порядок комунікації, автентифікацію, конфіденційність, обробку помилок і навіть таймінг – все, що має значення у справжньому світі. У таких завданнях викристалізовується зв'язок між алгоритмом і його місцем у загальній архітектурі захисту. Не менш важливою є участь у змаганнях формату CTF (Capture the Flag), де учасники повинні розв'язувати криптографічні головоломки, знаходити вразливості у фрагментах коду, розкодовувати зашифровані повідомлення. Це підвищує мотивацію, вчить працювати в команді та готує до реального практичного застосування знань у сфері кібербезпеки.

Таким чином, практичні завдання в криптографії – це не просто доповнення до теорії, а самостійна частина навчального процесу, яка дозволяє перевести знання у форму навичок. Вони формують здатність аналізувати, створювати та захищати, що і є кінцевою метою підготовки фахівця в цій сфері.

Міждисциплінарність у викладанні криптографії – це не просто згадка про суміжні дисципліни, а глибоке проникнення криптографії в інші наукові й практичні галузі, що робить її вивчення набагато ширшим за звичайне засвоєння алгоритмів. Власне, криптографія є точкою перетину математики, інформатики, інженерії, права, етики, а в сучасному цифровому світі – ще й політики та економіки. І тому її викладання неминуче вимагає міждисциплінарного підходу, який розширює світогляд студента й готує до реальних задач, що виходять за межі технічних обчислень.

Основи криптографії глибоко вкорінені в математиці, особливо в таких розділах як теорія чисел, комбінаторика, лінійна алгебра, теорія груп. Без розуміння модульної арифметики, досконалих чисел, простих чисел або дискретного логарифма неможливо збагнути механіку роботи таких алгоритмів, як RSA чи алгоритм Діффі-Геллмана. Але тут важливо не просто розглядати ці математичні теми ізольовано, а показувати, як вони прямо впливають на ефективність, криптостійкість і практичну реалізацію алгоритмів.

Паралельно, криптографія тісно переплетена з інформатикою. Це і алгоритми, і структури даних, і оптимізація, і розробка програмного забезпечення, де потрібно враховувати не лише теоретичну правильність, а й ефективність, безпеку в пам'яті, роботу з виключеннями, відповідність протоколам. Наприклад, під час написання цифрового підпису важливо не лише правильно реалізувати математичний алгоритм, а й забезпечити надійне зберігання приватного ключа в пам'яті, захист від побічних каналів, коректне форматування підпису відповідно до стандартів.

Іншою важливою площиною є право й регулювання. Студенти повинні розуміти, що використання криптографії регулюється законами: в деяких країнах застосування сильного шифрування обмежене, а зберігання або передача певного типу даних без шифрування – навпаки, є порушенням норм. Тут у гру вступає і цифрова етика: наскільки етично створювати

шифровані канали комунікації, які неможливо контролювати навіть у випадках загроз національній безпеці? Чи повинна держава мати «задні двері» до зашифрованих даних? Ці питання дають можливість інтегрувати філософські, соціальні й політичні аспекти в обговорення технічних тем. Не можна оминути увагою й економічну складову. Криптографія лежить в основі електронної комерції, банкінгу, криптовалют. Розуміння того, як працює блокчейн, як функціонують смарт-контракти, чому криптографія гарантує незворотність транзакцій – усе це допомагає краще оцінити, наскільки технічні знання впливають на сучасну економіку. Навіть психологія та UX-дизайн мають відношення до теми: складність паролів, впровадження двофакторної автентифікації, довіра користувачів до захищених сервісів – усе це залежить не лише від алгоритмів, а й від того, як люди їх сприймають і використовують.

Таким чином, міждисциплінарність не ускладнює викладання криптографії – вона робить його живим, наповненим реальним змістом. І найголовніше – вона готує студентів до ролі не лише технічних виконавців, а фахівців, здатних бачити ширший контекст і приймати обґрунтовані, відповідальні рішення.

Сучасні підходи до викладання криптографії суттєво змінилися порівняно з класичними моделями, орієнтованими переважно на лекційний формат і виклад математичної теорії. Сьогодні акцент зміщується на студент-орієнтоване навчання, розвиток практичних навичок, критичного мислення та роботу з реальними кейсами. Це зумовлено не лише зростанням складності інформаційного середовища, а й тим, що криптографія більше не є закритою галуззю – вона стала доступною, необхідною та інтегрованою у повсякденні технології, від месенджерів до банківських систем. Однією з ключових тенденцій є проєктно-орієнтоване навчання. Замість абстрактних задач студенти отримують конкретні кейси – наприклад, створити систему автентифікації користувача або симулювати протокол захищеного обміну ключами між сервером і клієнтом. Такий підхід стимулює самостійну дослідницьку діяльність, вміння працювати в команді, інтегрувати знання з різних дисциплін та шукати практичні рішення.

Ще один важливий напрям – використання інтерактивних інструментів. Онлайн-симулятори, візуалізації, лабораторії на базі Python, JavaScript або спеціалізованих платформ на кшталт CrypTool чи OverTheWire дозволяють студентам “помацати” алгоритми руками. Наприклад, замість простої формули студенти бачать, як змінюється текст на кожному етапі шифрування, як виглядає розподіл байтів у зашифрованому повідомленні чи як діє атака на повторне використання ключа.

Сучасна криптографія тісно пов’язана з актуальними подіями – витоками даних, шкідливими програмами, політичними скандалами, де цифрова безпека відіграє центральну роль. Тому дедалі частіше до навчального процесу інтегрують аналіз реальних інцидентів, які розбирають як кейси: що саме сталося, яка роль криптографії, де була вразливість, як можна було цього уникнути. Такий аналіз дає студентам не лише технічну, а й стратегічну перспективу.

Також набирає популярності підхід “навчання через змагання” – CTF (Capture The Flag), де криптографічні задачі вплітаються у формат квестів: учасники повинні знайти спосіб зламати шифр, декодувати повідомлення або знайти ключ. Такий формат поєднує елемент гри, змагальності й дослідження, що значно підвищує мотивацію.

Сучасне викладання криптографії також активно використовує принципи гнучкого навчання: студенти мають змогу обирати траєкторію – більше теорії для тих, хто прагне академічної глибини, або більше практики для тих, хто орієнтований на прикладні ІТ-рішення. Деякі курси дозволяють працювати з відкритими кодами, писати власні бібліотеки, вивчати стандарти (наприклад, RFC-документи) та навіть долучатися до розробки open-source проектів. Не менш важливим є розвиток так званої «криптографічної грамотності» – здатності не лише створювати або застосовувати алгоритми, а й критично оцінювати їхню доцільність, етичність та відповідність ситуації. Наприклад, коли і чому недостатньо просто шифрувати дані? Яка різниця між формальною безпекою і реальною, що залежить від людського фактору, середовища використання або економічних обмежень?

Таким чином, сучасні підходи до викладання криптографії орієнтовані на гнучкість, контекст, практичність і міждисциплінарність. Вони формують не лише знання, а й компетентності – здатність аналізувати, створювати і приймати рішення в реальному, швидкозмінному цифровому світі.

Отже, викладання криптографії сьогодні – це значно більше, ніж просто передача знань про алгоритми та математичні концепції. Воно перетворюється на комплексний освітній процес, що поєднує глибоку теоретичну базу з практичними навичками, залучає міждисциплінарний контекст і сучасні освітні технології. Ефективне навчання в цій галузі формує у студентів не лише технічну компетентність, а й критичне мислення, здатність адаптуватися до нових викликів цифрової безпеки та усвідомлення соціальної й етичної відповідальності. Саме такий підхід дозволяє готувати фахівців, які не просто володіють інструментами, а розуміють їх зміст, межі застосування та значення в сучасному світі.

ЛІТЕРАТУРА

1. Гевко І., Ящик О., Савчин Т., Гільтай Л. Кібербезпека в децентралізованій інтернет-екосистемі WEB 3.0. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. (2023). Серія: педагогіка, 1(1), 61–68. https://doi.org/10.25128/2415-3605.23.1.8/.
2. Crypto-Steganographic System based on the Solver of the Square Root of a Prime Number / Kukharska, N., Lagun, A., Yashchyk, O. Proceedings – International Conference on Advanced Computer Information Technologies, ACIT, 2024, pp. 535–538. DOI 10.1109/ACIT62333.2024.10712448.
3. Застосування технології блокчейн в інформаційній системі управління освітніми документами / Ожга М.М., Ящик О.Б. //Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи. Матеріали IX Міжнародної науково-практичної інтернет-конференції (м. Тернопіль, 28 квітня, 2022). – 31-33 с.
4. Ящик О., Твердохліб І., Франко Ю., Ожга М. Використання технології блокчейн для забезпечення автоматизації управління освітніми документами. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. (2022). Серія: педагогіка, 1(2), 113–120. – DOI: https://doi.org/10.25128/2415-3605.22.2.14.