вразливостями; 3) контроль привілейованих облікових записів; 4) сегментація IT/OT мереж; 5) аналіз журналів подій безпеки. Підхід «CIS Implementation Group 1» дозволяє ОКІ сформувати базову лінію захисту [2]. Особлива увага має приділятися механізмам MFA для віддаленого доступу до технологічних сегментів, що запобігає несанкціонованому втручанню в системи керування.

Висновки. Впровадження пріоритетних контролів безпеки стратегічно важливе для стійкості ОКІ, оскільки оптимізує витрати та прискорює реагування на інциденти. Подальші дослідження будуть спрямовані на автоматизацію перевірки відповідності цим контролям у реальному часі.

1. Сіденко В. П., Гнатюк С. О. Метод підвищення рівня захищеності критичних інформаційних систем держави. Кібербезпека: освіта, наука, техніка. – 2024. – Т. 4, № 24. – С. 138–154.
2. CIS Critical Security Controls Version 8. Center for Internet Security, 2021. 82 p.

Дослідження методів побудови постквантових крипто-кодових конструкцій на гіпереліптичних кодах

УДК 621.395.7 (043.2)

Сергій Євсеєв[1], Владислав Сокол[2]

Національний технічний університет «Харківський політехнічний інститут», [1]Serhii.Yevseiev@gmail.com, [2]Vladyslav.sokol@gmail.com

Фундаментальний зсув парадигми інформаційної безпеки у напрямку постквантової криптографії стимулює інтенсивний пошук нових алгебраїчних структур. Дослідження фундаментальних аспектів застосування гіпереліптичних кривих у сучасних системах криптографічного захисту інформації, наведені у [1], показують багатообіцяючі результати. Доведено, що такі багатовимірні алгебраїчні структури здатні забезпечити надзвичайно високий рівень безпеки при використанні значно коротших ключів порівняно з традиційними еліптичними аналогами завдяки більшій розмірності групи класів дивізорів нульового степеня. Але залишилися невирішеними питання, пов'язані з алгоритмічним забезпеченням швидкого та детермінованого підрахунку кількості раціональних точок для кривих довільного роду над довільними полями Галуа. Причиною цього явища виступають суттєві об’єктивні математичні труднощі, безпосередньо пов’язані з неминучим експоненційним зростанням обчислювальної складності в процесі безпосереднього розрахунку порядку Якобіана для складних типів кривих. Специфіка імплементації суворих методів багатофакторної автентифікації на основі модифікованих крипто-кодових систем у фінансовому секторі формалізована у [2]. Встановлено, що глибоко інтегровані механізми захисту, які органічно поєднують завадостійкість та криптографічну конфіденційність, є критично необхідними для безпечного проведення віддалених банківських транзакцій в умовах гібридних кіберзагроз. Але залишилися невирішеними питання, пов'язані з оптимізацією пропускної здатності комунікаційного каналу під час постійної передачі автентифікаційних токенів надто великого розміру. Варіантом

подолання відповідних труднощів може бути повна відмова від традиційних плоских структур та перехід до використання кодів з екстремально високою алгебраїчною щільністю та багатовимірною просторовою геометрією. Саме такий підхід логічно випливає з результатів аналізу, проте практичні методики побудови перевірочних матриць безпосередньо з Якобіанів гіпереліптичних кривих у науковій літературі досі не формалізовані. Все це дозволяє стверджувати, що доцільним є проведення дослідження, присвяченого побудові та аналізу алгебро-геометричних кодів на базі гіпереліптичних кривих над полем Галуа. Фундаментальною основою синтезованих крипто-кодових конструкцій виступає математичний апарат алгебраїчної геометрії [3]. Скінченне поле Галуа $GF(2^m)$ строго задається за допомогою незвідного полінома f(x) та канонічного базису елементів 1, x, x^2, …, x^{m-1}. Для виконання процедур серіалізації бітових векторів у системі застосовується цілочисельне кодування вигляду

$$v = \sum_{i=0}^{m-1} v_i 2^i. \quad (1)$$

Гіпереліптична крива C роду g над полем $GF(2^m)$ задається рівнянням у загальній формі

$$C: y^2 + h(x)y = f(x), \quad (2)$$

де $h(x) \in GF(2^m)[x]$ є поліномом зі степенем $\deg(h) \le g$, а $f(x) \in GF(2^m)[x]$ виступає нормованим поліномом степеня $\deg(f) = 2g+1$ або $\deg(f) = 2g+2$. Критичною вимогою для криптографічного застосування є відсутність сингулярних точок, що означає неможливість існування розв'язків $(x, y) \in \overline{GF\left(2^m\right)} \times \overline{GF\left(2^m\right)}$, які б одночасно задовольняли базовому рівнянню C та системі його часткових похідних [4].

У процесі синтезу архітектури сформовано математичну модель алгебро-геометричного коду на базі гіпереліптичної кривої. У явному вигляді модель детерміновано кортежем параметрів $M = (GF(2^m), C, P_{rat}, E_L, H, G)$. Елемент C задає рівняння кривої (2), а P_{rat} – множину проєктивних точок (4). Матриці E_L, H та G визначають межі кодового простору. Запропонована формалізація адаптує топологічні властивості многовидів до формату дискретних структур даних [1]. Застосована у дослідженні трансформація координат повністю та остаточно розв'язала цю алгоритмічну проблему. Відображення кожної скінченної афінної точки у систему проєктивних координат із введенням додаткової просторової змінної дозволило звести рівняння кривої до гомогенної (однорідної) форми. Здійснено імплементацію згенерованих гіпереліптичних кодів у дві фундаментальні теоретико-кодові архітектури: асиметричну схему Мак-Еліса (McEliece) та симетричну схему Рао-Нама (Rao-Nam). Встановлено, що класична асиметрична парадигма з жорстким табличним декодером вимагає виконання $O(k^2)$ операцій на розв'язання лінійних систем відносно відкритого тексту та провокує експоненційне зростання обсягів оперативної пам'яті. Натомість інтеграція алгебро-геометричного коду в симетричну канальну архітектуру з використанням криптографічного генератора псевдовипадкових чисел для формування маски штучної помилки дозволила повністю обійти етап обернення щільних матриць.

1. Alimoradi, R. (2016). A Study of Hyperelliptic Curves in Cryptography. IJCNIS, 8(8), 67–72. https://doi.org/10.5815/ijcnis.2016.08.08
2. Yevseiev, S., Kots, H., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6(4(84)), 11–23. https://doi.org/10.15587/1729-4061.2016.86175.
3. Hubrechts, H. (2011). MEMORY EFFICIENT HYPERELLIPTIC CURVE POINT COUNTING. Int. J. Number Theory, 07(01), 203–214. https://doi.org/10.1142/S1793042111004034.
4. Conceição, R. (2020). ON INTEGRAL POINTS ON ISOTRIVIAL ELLIPTIC CURVES OVER FUNCTION FIELDS. Bull. Aust. Math. Soc., 102(2), 177–185. https://doi.org/10.1017/S0004972720000155

Дослідження методів та засобів ідентифікації дезінформативних новин у соціальних мережах

УДК 004.8:004.7

Тарас Труш[1], Марія Стадник[2]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]tarastrush.dev@gmail.com, [2]stadnyk_m@tntu.edu.ua

У період стрімкої цифровізації суспільства соціальні мережі стали ключовим джерелом поширення інформації, але водночас є інструментом для навмисного поширення дезінформації. Досвід України, яка з 2014 року опинилася серед перших держав, що зіткнулися з масштабними дезінформаційними кампаніями в соціальних мережах, демонструє, що ця проблема переросла у фактор загрози національній безпеці. Фейкові профілі, ботоферми, маніпулятивні матеріали та синтетичний медіаконтент активно використовуються як інструменти гібридної війни. Додатковим викликом є швидкий розвиток генеративного штучного інтелекту, який значно ускладнює відокремлення правдивої інформації від неправдивої. У зв'язку з цим зростає потреба у створенні дієвих автоматизованих систем виявлення дезінформації.

Метою дослідження є аналіз сучасних методів автоматизованої детекції дезінформації в соціальних мережах та оцінка ефективності гібридних і мультимодальних підходів для виявлення маніпулятивного контенту. Поширення дезінформації в соціальних мережах та розвиток генеративного штучного інтелекту створюють серйозні загрози інформаційній безпеці. Сучасні методи виявлення фейкової інформації потребують поєднання текстового, візуального та мережевого аналізу, однак україномовний інформаційний простір залишається недостатньо дослідженим.

На основі аналізу публікацій з баз даних Scopus, Web of Science, Google Scholar та arXiv за 2017–2025 роки встановлено, що методи детекції дезінформації поділяються на три основні категорії. Контент-орієнтовані підходи базуються на аналізі текстових та візуальних ознак новин із використанням NLP-технік і трансформерних моделей (BERT, RoBERTa, DeBERTa) [1]. Мультимодальні методи поєднують обробку тексту та зображень