ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

КРИПТОЛОГІЯ / CRYPTOLOGY

DOI: 10.18372/2225-5036.28.16953

АНАЛІЗ ЗАСТОСУВАННЯ ГІБРИДНИХ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ ДЛЯ ПІДВИЩЕННЯ РІВНЯ СТІЙКОСТІ ГЕШ-КОДІВ ДО ЗЛАМУ

Алла Гаврилова[1], Юлія Хохлачова[2], Володимир Погорелов[3]

[1] Національний технічний університет "Харківський політехнічний інститут", Україна
[2, 3] Національний авіаційний університет, Україна

ГАВРИЛОВА Алла Андріївна, старший викладач кафедри кібербезпеки
Рік та місце народження: 1972, м. Молодогвардійськ, Краснодонський район, Луганська область, Україна.
Освіта: Харківський національний економічний університет, 1994.
Посада: старший викладач кафедри кібербезпеки Національний технічний університет "Харківський політехнічний інститут", Україна.
Наукові інтереси: криптографічні методи захисту інформації в телекомунікаційних системах.
Публікації: більше 30 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: alla.havrylova@khpi.edu.ua**.**
ORCID ID: 0000-0002-2015-8927.

ХОХЛАЧОВА Юлія Євгеніївна, к.т.н., доцент.
Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, оцінювання уразливостей, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: yuliiahohlachova@gmail.com.
ORCID ID: 0000-0002-1883-8704.

ПОГОРЕЛОВ Володимир Володимирович, к.т.н.,
Рік та місце народження: 1990 рік, м. Київ, Україна.
Освіта: НТУУ «КПІ ім. І. Сікорського», 2014 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2018 року.
Наукові інтереси: методи і засоби захисту інформації, машинне навчання у задачах захисту інформації, генерування псевдовипадкових чисел та послідовностей, проектування комплексних систем захисту інформації, комп'ютерні віруси.
Публікації: понад 20 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: volodymyr.pogorelov@gmail.com.
ORCID ID: 0000-0002-6100-1504.

Анотація. *У статті представлено новий спосіб підвищення крипостійкості MAC-кодів повідомлень, що передаються через Інтерне-мережі. На сьогодні це має дозволити протистояти не тільки наслідкам комплексування кіберзагроз а й підвищенню швидкості несанкціонованого доступу до даних через створення таких нових апаратних можливостей, як квантова комп'ютерна технік. В роботі пропонується розгляд застосування модифікованого алгоритму UMAC на модифікованих еліптичних кривих Мак-Еліса із використанням криптокодових конструкцій з ознаками гібридності. Проведено перевірку запропонованих конструкцій на колізійні властивості. Для цього було розроблено програмний додаток в середовищі об'єктно-орієнтованої мови*

програмування C#. Для виявлення можливостей геш-кодів, що досліджувалися, з точки зору їх стійкості до зламування, цінності даних, у захисті яких вони повинні застосовуватися та з врахуванням безпечного часу до можливого зламування, було розроблено комплексний показник ефективності модифікованого алгоритму UMAC. У якості метода оцінки даного показника було запропоновано використовувати метод багатофакторного комплексного аналізу. Для цього були розроблені шкали вимірювання та інтерпретації кожного показника. Доведено, що даний метод оцінки дозволяє отримати достатньо адекватні результати та поєднати їх з результатами точних розрахунків за окремими параметрами. Також було досліджено питання зниження енергетичних витрат для формування крипто-кодових конструкцій, за результатами якого було доведено, що створення саме гібридних крипто-кодових конструкцій призводить до найменших енергетичних витрат.

Ключові слова: *автентифікація, криптостійкість, MAC-код, алгоритм UMAC, крипто-кодові конструкції, EC, MEC, DC, цінність інформації, безпечний час.*

Постановка проблеми

Зловмисники без зволікання приступили до пошуку вразливостей в сервісах на периметрах компаній, в тому числі в рішеннях, які використовуються для організації віддаленої роботи, перевіряючи їх на міцність. Так, активно експлуатувалися бекдори в Pulse Secure VPN, Citrix ADC і Citrix Gateway, в міжмережевому екрані Cisco ASA. Оператори програм-вимагачів, зокрема Netwalker, Clop і REvil, користувалися уразливими сервісами для поширення свого шкідливого програмного забезпечення (ПЗ). У зв'язку з цим актуальним є дослідження світових тенденцій кібербезпеки та визначення стану з цього питання в Україні. Найбільша частка злочинів, які вчиняються за допомогою Інтернет-мереж приходиться на державний і фінансовий сектор. До передових інформаційних технологій сьогодення проявляється інтерес не тільки із наукової зацікавленості чи у пошуках вирішення найважливіших задач людства, а й через пошук шляхів швидкого збагачення за рахунок фізичних осіб, різного рівня бізнес-структур, для проведення дистанційного шпіонажу та для нанесення збитків через несанкціоноване отримання доступу до критично важливої інфраструктури, даних, а також спотворення та крадіжки інформації.

Якщо досліджувати виток банківського сектору, то можна відмітити, що в останнє десятиріччя було значно розширено спектр послуг завдяки використанню обчислювальних ресурсів Інтернет-технологій та технологій X"G"–LTE (Long-Term Evolution).

Дані зміни визначили введення поняття цифрової економіки та подальший розвиток електронного банкінгу. [1, 2]. Разом з тим, в [3-5] представлено аналіз кіберзагроз за останні три роки (рис. 1) на автоматизовані банківські системи (АБС) організацій банківського сектору (ОБС).

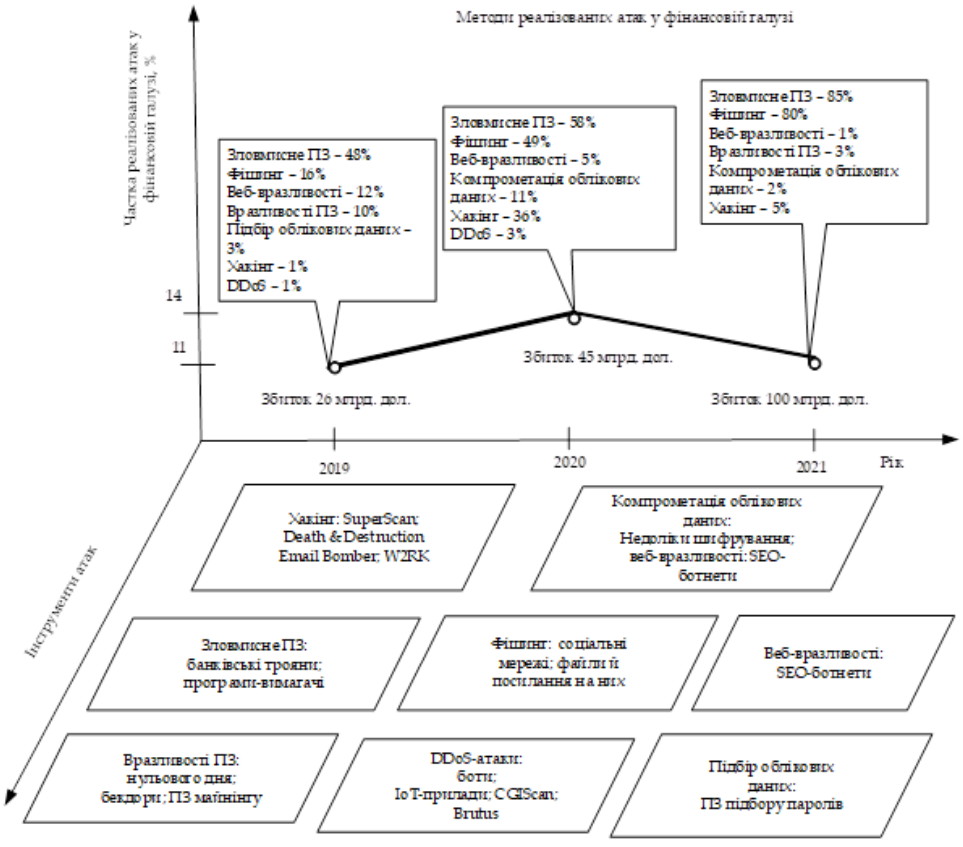

Рис.1. Тенденції напрямку кібератак на фінансовий сектор

Наведений графік показує, що за 2019-2021 роки на розміри збитків від реалізованих атак у фінансовому секторі значний вплив мали такі методи реалізованих атак як фішинг (2019 рік – 16%, 2020 рік – 49%, 2021 рік – 80%) та зловмисне забезпечення (ПЗ) (2019 рік – 48%, 2020 рік – 58%, 2021 рік – 85%). З погляду основних векторів сучасних атак на АБС проведений аналіз свідчить про їхнє комплексування з методами соціальної інженерії. Це призводить до появи у вже відомих загроз властивостей гібридності та синергізму [3-5]. Представлена статистка свідчить про те, що зростання загроз, пов'язаних із послугою автентичності, невпинно зростає.

Крім того, в роботах [6-15], розглянуто можливості повномасштабних квантових комп'ютерів, що забезпечують завдання зламування алгоритмів симетричної та несиметричної криптографії за поліноміальний час.

Таким чином, реалізація атаки на квантовому комп'ютері практично ставить під сумнів й стійкість алгоритмів гешування на основі блочно-симетричних шифрів в режимах CBC (Cipher Block Chaining) та CFB (Cipher Feedback Mode).

Якщо розглянути ситуацію, стосовно державних інформаційних ресурсів та об'єктів критичної інфраструктури, то на їх системи кіберзахисту згідно з моніторингом за період з початку грудня 2020 р. до кінця листопада 2021 р. було зафіксовано більше ніж 50 млн. підозрілих подій, біля 2 млн. атак різних видів та до 100 тис. кіберінцидентів [16] (рис. 2-4).

Також за цей період зафіксовано і заблоковано понад 500 DDoS-атак, зокрема на веб-ресурси Офісу Президента України та Держспецзв'язку.

Дані тенденції характерні й для кіберпростору по всьому світові. Так, в атаках на організації основними векторами доставки шкідливого програмного забезпечення (ПЗ) залишаються електронна пошта (71 %) і компрометація комп'ютерів, серверів та мережевого обладнання (24 %), а в атаках на приватних осіб хакери віддають перевагу. електронній пошті і веб-сайтам (по 32%) [17].

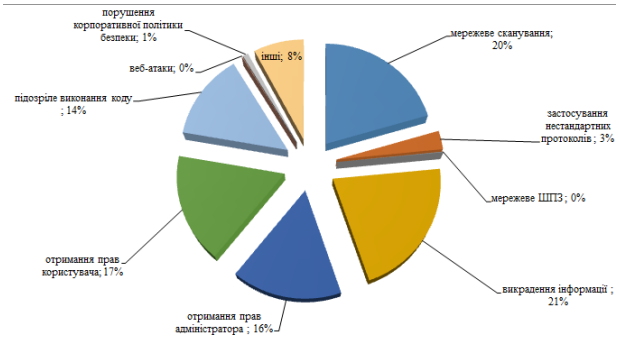

Рис. 2. Група «Підозрілі події» за об'єктами моніторингу

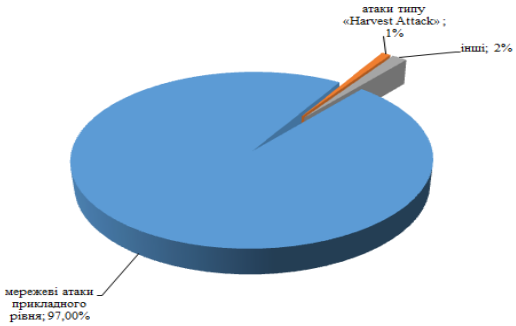

Рис. 3. Група «Кібератаки» за доступом державних органів до мережі Інтернет

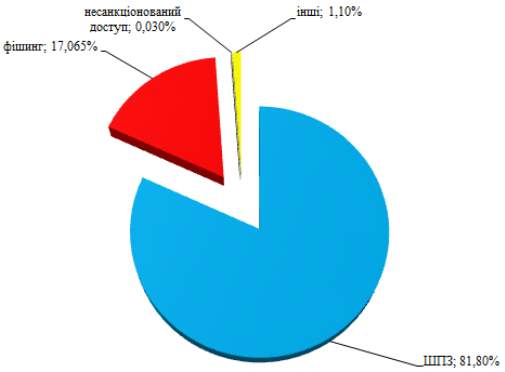

Рис. 4. Група «Кіберінциденти» за об'єктами моніторингу

Виходячи із наведених статистичних даних, можна зазначити, що основним джерелом виникнення кіберінцидентів є канали передачі інформації, в тому числі й електронна пошта. При автентифікації користувачів в електронній пошті використовується гешування паролів, яке проводиться з використанням алгоритму криптографічного захисту MD5. Але, за умов роботи в постквантовому періоді, даний алгоритм не володіє необхідною криптостійкістю до зламування, тому постає завдання створення нових алгоритмів або модифікації вже наявних. Інтенсивний розвиток інформатизації призвів також і до зростання кількості інформаційних систем (ІС) різного призначення. Кількість зареєстрованих суб'єктів і об'єктів в ІС величезна. До складу таких ІС входять й великі бази даних (Big Data), що призвело до створення великих інформаційними системами (ВІС). Кількість ВІС збільшується. Цьому сприяє розвиток таких технологій, як технології інтернет-речей (Internet of Things, IoT) і блокчейн технології. Якщо до блокчейн технології, то з точки зору не тільки її використання, як платформи для роботи з криптовалютою, але й як антикорупційного механізму, на сьогодні в Україні вже реалізовано ряд таких проєктів [18, 19], а саме:

– електронні аукціони, які являють собою онлайн-аукціони в державних галузях, які дозволяють здавати в оренду державне майно;

– відкрита платформа електронної демократії E-vox розроблена для використання блокчейн в організації голосувань, референдумів, підписання петицій, причому голосування проводиться безпосередньо зі своїх смартфонів і планшетів, залишаючи запис в блокчейн;

– блокчейн в Національному банку України (НБУ), введений як дорожня мапа розвитку безготівкової економіки, і являє собою випуск електронних грошей на базі блокчейн в рамках розвитку національної платіжної системи "простір";

– електронний уряд E-Ukraine, який являє собою портал, що є місцем взаємодії громадян, бізнесу та держави, й об'єднує на одній платформі аукціони, голосування, ведення держреєстрів і інші розподілені сервіси;

– банки на блокчейн реалізовані за допомогою розподіленої банківської системи Smart Money, яка дозволяє будувати інфраструктуру для операцій з електронними грошима;

– електронна гривня (е-гривня – є дослідним проєктом), що є електронними грошима, не прив'язаними до жодної фінансової установи, і представляє собою систему моментальних веб-розрахунків;

– Державний земельний кадастр, який є реєстром автобусних перевезень і реєстром інвестиційних проєктів у сфері інфраструктури.

Але при забезпеченні дистанційної електронної взаємодії важливим є забезпечення процесу розпізнавання об'єкта за пред'явленими параметрами (ідентифікаторами) і пов'язаного з ним процесу автентифікації. Найбільш гостро це завдання повстає в системах управління доступом і підтвердження автентифікації і верифікації при передачі повідомлень [20]. При постійному збільшенні зростання кібератак і різного роду шахрайств, питання ідентифікації відправника і одержувача при їх взаємодії стають особливо актуальними. При забезпеченні підвищення криптостійкості алгоритмів шифрування повідомлень для передачі по каналах зв'язку, використовуються системи симетричного і асиметричного шифрування. Алгоритм RSA (Rivest, Shamir, Adleman), заснований на еліптичних кривих і обчислювальної складності задачі факторизації великих чисел, на сьогодні, забезпечує високу криптостійкість переданих повідомлень, за рахунок неможливості за обчислювальний час провести розшифрування цих повідомлень. Але даний алгоритм стійкий лише при існуючих обчислювальних потужностях, а при появі високопродуктивних квантових комп'ютерів збільшиться й ризик його зламування.

Тому, згідно із майбутніми змінами в технічному оснащенні зловмисників та появою квантового комп'ютеру, важливим напрямком у розвитку постквантової криптографії сьогодні є дослідження крипто-кодових системи (конструкції). Їх формування засноване на використанні алгебраїчних кодів, замаскованих під так званий випадковий код [21, 22]. Такі конструкції мають дозволити інтегровано реалізувати швидке криптографічне перетворення даних і забезпечити достовірність даних, що передаються на основі завадостійкого кодування [22, 23].

Аналіз останніх досліджень і публікацій

В межах розв'язання задачі цілісності інформації використовуються криптографічні методи, за допомогою яких можна виявляти не лише випадкові спотворення інформації, а й її цілеспрямовану зміну. Так, процес контролю цілісності забезпечується за рахунок введення в передану інформацію надмірності - перевірочної комбінації байт [26]. Така комбінація байт обчислюється згідно з алгоритмами [27], за якими перевіряється, чи були дані змінені несанкціоновано і яка міра імітостійкості шифру.

В умовах зростання обчислювальних ресурсів та сучасних технологій збільшення обсягів даних виникає інтегроване завдання забезпечення не лише безпеки, оперативності, а й автентичності. Для виконання пропонується використовувати алгоритм каскадного гешування UMAC, який дозволяє забезпечити необхідний рівень стійкості та оперативності на основі використання універсальних функцій гешування. Однак, класична схема для забезпечення стійкості геш-коду використовує алгоритм блочно-симетричного шифру AES, що не дозволяє забезпечити універсальність.

В роботах [28, 29] розглянуто можливість побудови каскадного алгоритму UMAC на основі використання безключових алгоритмів MASH-1 та MASH-2 у ролі псевдовипадкової підложки на третьому шарі. Однак, наведені авторами результати свідчать про те, що алгоритм MASH-1 не забезпечує необхідних параметрів стійкості та універсальності і не може використовуватися в модифікованому (удосконаленому) алгоритмі. У роботі [30] розглянуто алгоритми формування геш-функцій на основі використання циклічних алгеброгеометричних завадостійких кодів. Такий підхід забезпечує універсальність і дозволяє використовувати крипто-кодові конструкції як псевдовипадкову підложку в каскадному алгоритмі гешування.

В роботах [7, 10, 31] розглянуто гібридні криптокодові конструкції (ГККК) на основі синтезу класичних схем Мак-Еліса та Нідеррайтера. Однак використання двох схем збільшує не тільки ємнісні витрат на її практичну реалізацію, а й знижує оперативність криптоперетворень, що є істотним для використання при формуванні МАС-коду.

У роботі [32] автори розглядають використання циклічних кодів Ріда-Соломона, проте не проводять дослідження стійкості такої крипто-кодової конструкції до атаки Сидельникова, що не дозволяє використовувати ККК як "гарант" стійкості геш-коду.

У роботі [33] розглянуто можливість використання крипто-кодової конструкції Нідеррайтера в постквантовій криптографії, проте дана схема використовує два алгоритми (рівноважного кодування та схеми Мак-Еліса), що ускладнює формування псевдопідложки та практичну реалізацію.

В роботах [34, 35] розглянуто стійкість універсальних геш-функцій. Автори підтверджують, що використання універсального гешування не дозволяє однозначно формувати стійкі до зламування геш-коди, і пропоную використовувати додаткове шифрування для забезпечення стійкості геш-коду.

У роботі [36] пропонується використання нової схеми багатоадресної автентифікації з урахуванням симетричного алгоритму. Однак, в умовах постквантового періоду, даний алгоритм може бути зламаний, а використання модифікованого каскадного алгоритму гешування забезпечить необхідний рівень стійкості та оперативності. Таким чином, формування модифікованого алгоритму UMAC на основі крипто-кодових конструкцій забезпечить вирішення задачі автентифікації в умовах постквантової криптографії та подальшого зростання інформаційних масивів даних. Проведений аналіз можливостей криптоаналізу в роботі [24] підтверджує, що на основі квантових

алгоритмів Шора та Гровера, та повномасштабного квантового комп'ютера, алгоритми симетричної та несиметричної криптографії схильні до зламування за поліноміальний час.

В роботах [7–10] відзначається перспективний напрямок – використання крипто-кодових конструкцій (ККК) Мак-Еліса та Нідеррайтера. Їх використання забезпечує необхідну швидкість кодування на рівні симетричних алгоритмів та формування несиметричної криптосистеми. Істотними недоліками їх практичного використання є можливість знаходження елементів матриць маскування (особистого ключа кожного користувача системи) на основі атаки Сидельникова [25] та значних енергетичних витрат на практичну реалізацію над обчислювальним полем розмірністю GF (2^{10}–2^{13}).

Таким чином, актуальним завданням на сьогодні є розробка модифікованого алгоритму UMAC на основі крипто-кодових конструкцій Мак-Еліса.

Основні матеріали дослідження

Згідно з проведеним аналізом проблем систем кіберзахисту в фінансовому та державному секторах, можна зробити висновок про те, що необхідно підвищувати криптостійкість кодів автентифікації повідомлень, що передаються каналами телекомунікацій. Це можна зробити за допомогою проведення модифікаційних змін у формуванні геш-кодів. В даній роботі запропоновано використовувати модифікований алгоритм UMAC на еліптичних кривих Мак-Еліса з використанням крипто-кодових конструкцій.

Тому рекомендовано використовувати геш-коди, сформовані таким чином, у якості індексів бази даних в Big Data та для передачі даних за запитом телекомунікаційними каналами зв'язку. Перетворене таким способом криптографічне перетворення можна представити в загальному вигляді як такий кортеж [1, 23, 37 – 40.]:

$$\{C_{Index/mess}; Hash_{UMAC}; Pad\}, \qquad (1)$$

де $C_{Index/mess}$ – кодограма індексу / повідомлення;
$Hash_{UMAC}$ – геш-код індекса/повідомлення;
Pad – псевдовипадкова підложка.

Для визначення потенційних можливостей запропонованих перетворень та доцільності їх використання при передачі через Інтернет, необхідно дослідити та проаналізувати наступне: 1) особливості формування різних видів модифікацій крипто-кодових конструкцій; 2) проаналізувати колізійні властивості модифікацій крипто-кодових конструкцій за методиками універсальності та суворої універсальності формування геш-кодів; 3) оцінити практичну реалізацію колізійних властивостей геш-кодів; 4) оцінити ефективність використання модифікованого алгоритму UMAC за розглянутими крипто-кодовими перетвореннями за певними критеріями й умовами, що висуваються.

1) особливості формування різних видів модифікацій крипто-кодових конструкцій.

При використанні надійної геш-функції обчислювально складно створити підроблене повідомлення з таким самим значенням геш-коду (МАС-код – message authentication code), як у справжнього повідомлення. Однак ці загрози можуть реалізуватися через слабкість конкретних алгоритмів гешування, підпису або помилок у їх реалізації [1, 37].

Доцільним є спосіб побудови багатошарових гешуючих функцій за прикладом алгоритму UMAC. Він базується на поєднанні багатоетапного ключового універсального гешування та використання блочного симетричного шифру.

Даний алгоритм використовує безліч універсальних геш-функцій і забезпечує доведену безпеку при формуванні коду автентифікації [2, 38]:

1 шар – значення універсальної геш-функції (UHASH-hash) першого рівня гешування:

$$Y_{L1} = Hash_{L1}(K_{L1}, M_{index/mess}), \qquad (2)$$

де $M_{index/mess}$ – індекс / повідомлення;

$Hash_{L1}$ – функція ключового універсального гешування $M_{index/mess}$ з використанням секретного ключа першого рівня гешування K_{L1};

2 шар – значення універсальної геш-функції (UHASH-hash) другого рівня гешування:

$$Y_{L2} = Hash_{L2}(K_{L2}, Y_{L1}), \qquad (3)$$

де $Hash_{L2}$ – функція ключового універсального гешування Y_{L1} з використанням секретного ключа другого рівня гешування K_{L2};

3 шар – значення універсальної геш-функції (UHASH-hash) третього рівня гешування:

$$Y_{L3} = \left(\left(\left(\sum_{i=1}^{m} Y_{L2_i} K_{L3_{1i}}\right) \bmod(prime(36))\right) \bmod(2^{32})\right) xor(K_{L3_2}), \qquad (4)$$

де xor – операція "Виключного АБО" над попереднім та наступним значеннями.

Додаткову криптостійкість коду надає використання на останньому шарі псевдовипадкової підложки *Pad* [6, 7, 8, 39]:

$$Y = Hash_{UMAC} \oplus Pad. \qquad (5)$$

Таким чином, універсальне гешування в багатошаровій конструкції UMAC дозволяє забезпечити однакову ймовірність формування геш-образів для безлічі використовуваних ключових даних (рис. 5). Ця властивість і забезпечує безпеку алгоритму [40, 41] шифрування.

Псевдовипадкова підложка *Pad* посилює криптостійкість коду автентифікації МАС. Формування псевдовипадкової підложки *Pad* представляється у вигляді гібридних крипто-кодових конструкцій Мак-Еліса на модифікованих еліптичних кривих (МЕС) з різними видами модифікацій (на подовжених та укорочених, а також збиткових кодах) [40].

Для формування *Pad* у вигляді крипто-кодових конструкцій на модифікованих еліптичних кодах з подовженням та укороченням та у вигляді гібридних крипто-кодових конструкцій на модифікованих еліптичних кодах з нанесенням збитку (DC) [38]:

- формування множини збиткових текстів *CFT:*

$$CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\}; \qquad (6)$$

- формування множини збитків *CHD:*

$$CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\}; \qquad (7)$$

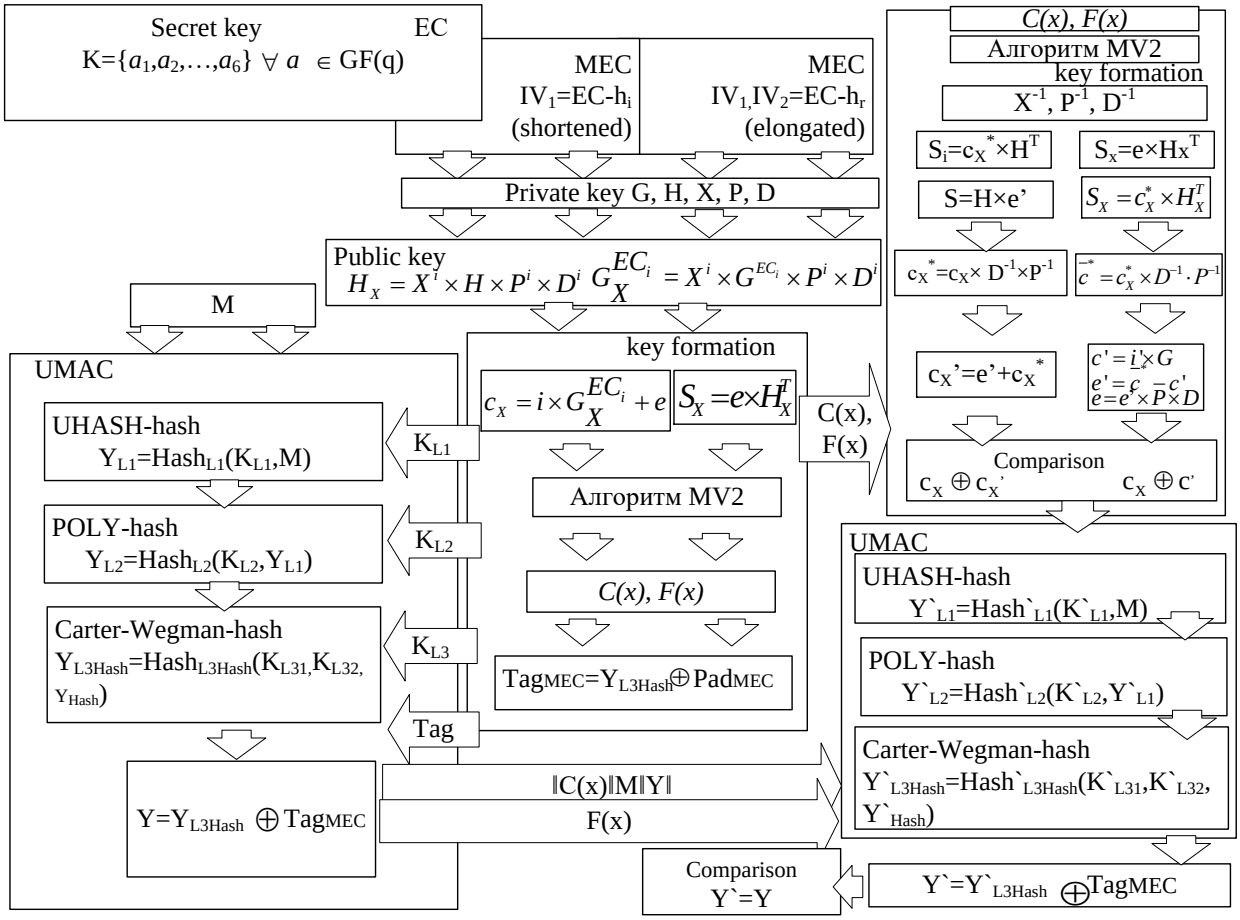

Рис. 5. Структурна схема реалізації модифікованого алгоритму UMAC на гібридних крипто-кодових конструкціях (KKK) Мак-Еліса і Нідеррайтера на еліптичних кодах (EC), на модифікованих еліптичних кодах (MEC) й на збиткових кодах (DC)

- формування множини прямого нанесення збитку (базуючись на використанні ключа – K^i_{MV2}, і алгоритму *MV*2):

$$E=\{E^1_{K_{MV2}},E^2_{K_{MV2}},...,\phi^S_{K_{MV2}}\}, \quad (8)$$
$$i=1,2,...,s;$$

- формування множини відображень *MV2* F^r_n задається об'єктивним відображенням між множиною перестановок $\{S_1,S_2,...,S_{2^n}\}$ та множиною $\#F^r_n$, $\#F^r_n=\#\{(c,f)\}=2^n!$;

- формування множини осмисленого тексту (базуючись на використанні ключа – K^i_{MV2}, і алгоритму *MV*2):

$$E^{-1}=\{E^1_{K_{MV2}}{}^{-1},E^2_{K_{MV2}}{}^{-1},...,E^S_{K_{MV2}}{}^{-1}\}, \quad (9)$$
$$E^{-1}_{K_{MV2}}:\|f(x)_i\|+\|C(x)_i\|\to M,\ i=1,2,...,s,$$

де y – деякий параметр, $y\in_Y Z_{q^m}$; $f(x)_i$ – прапор (збиток, *CHD*), $C(x)_i$ – залишок (збитковий текст, *CFT*); $f(x)=n-|C(x)|$, якщо $|C(x)|>y$, де y – деякий параметр, $y\in_Y Z_{q^m}$, $0<y<n$;

- формування множини ключів перетворення збиткових кодів:

$$K^i_{MV2}\in K_{MV2}; \quad (10)$$

- формування тексту з нанесенням модифікацій (подовження/укорочення, збиток):

$$C^*_j=C_j-C_{k-h_j},E_{K_{MV2}}, \quad (11)$$

$$C^*_j=C_{h_r},E_{K_{MV2}}, \quad (12)$$

де C_j – кодограма індексу/повідомлення;

C_{k-h_j} – модифікований код індексу/повідомлення при укороченні;

C_{h_r} – модифікований код індексу/повідомлення при подовженні;

$E_{K_{MV2}}$ – збиток на основі використання ключа K^i_{MV2} та алгоритму *MV*2.

Таким чином, як механізм формування псевдовипадкової підложки *Pad* для третього шару каскадного алгоритму гешування UMAC, пропонується використовувати крипто-кодові конструкції на еліптичних кривих та її модифікаціях.

2) проведення аналізу колізійних властивостей модифікацій крипто-кодових конструкцій за методиками універсальності та суворої універсальності формування геш-кодів.

В роботах [42, 43] було запропоновано використовувати методику універсальності та суворої універсальності для перевірки геш-кодів на їх колізійні властивості. За допомогою цієї методики запропоновано перевіряти геш-коди, сформовані за допомогою модифікованого алгоритму UMAC. Формалізоване уявлення цієї методики дозволяє розробити практичний алгоритм її реалізації. Розглянемо алгоритми пере-

вірки геш-кодів на можливість виникнення колізій за критеріями універсальності та суворої універсальності.

а) *алгоритм перевірки геш-кодів виконання вимог універсального класу геш-функцій* полягає у реалізації наступних кроків.

Крок 1. Формуються вхідні повідомлення $I_1, I_2, \ldots, I_j \in I$.

Крок 2. Формуються ключі $K_1, K_2, \ldots, K_j \in K$.

Крок 3. За кожним вхідним повідомленням I_i із застосуванням ключів K_j формують їх геш-коди H_{ij}.

Крок 4. Проводимо послідовне порівняння отриманих геш-кодів H_{ij} за однаковим ключем K_j за всіма вхідними повідомленнями між собою і з врахуванням наступної умови:

якщо значення геш-кодів співпадають ($H_{ij} = H_{ij+1}$), то це свідчить про виникнення колізії (L_j), і до лічильника колізій додається 1:

$$L_j = \sum_{j=1}^{N} L_{j-1} + 1, \qquad (13)$$

де L_{j-1} – попереднє значення лічільника колізій за j-им ключем.

Крок 5. В рамках одного повідомлення за всіма ключами обираємо максимальне значення колізій L_{maxi}.

Крок 6. Розраховуємо середнє арифметичне або центральне значення за максимумами кількості колізій шляхом знаходження їх математичного очікування $M(L_{maxi})$:

$$M\left(L\max_i\right) = \sum_{i=1}^{M} x_i \times p_i. \qquad (14)$$

Крок 7. Розраховуємо значення розкиду максимальних значень колізій навколо їхнього центрального значення шляхом знаходження дисперсії ($D(L_{maxi})$) за максимумами кількості колізій:

$$D\left(L\max_i\right) = M\left(x - M\left(x\right)\right)^2. \qquad (15)$$

б) *алгоритм перевірки геш-кодів на виконання вимог суворо універсального класу геш-функцій за першим критерієм* полягає у реалізації наступних кроків.

Крок 1. Формуємо одне випадкове вхідне повідомлення $I_{случ}$.

Крок 2. Формуємо геш-код $H_{случ}$ випадкового повідомлення $I_{случ}$.

Крок 3. Формуємо вхідне повідомлення $I_1, I_2, \ldots, I_j \in I$.

Крок 4. Формуємо ключі $K_1, K_1, \ldots, K_j \in K$.

Крок 5. За кожним вхідним повідомленням I_i із застосуванням ключів K_j формуємо їх геш-коди H_{ij}.

Крок 6. Проводимо послідовне порівняння отриманих геш-кодів H_{ij} за однаковим ключем K_j за всіма вхідними повідомленнями із геш-кодом $H_{случ}$ випадкового повідомлення $I_{случ}$ із застосуванням наступної вимоги: якщо значення геш-кодів співпадають ($H_{ij} = H_{случ}$), то це свідчить про виникнення колізій (L_j), тоді до лічильника колізій додається 1 (13).

Крок 7. В межах одного повідомлення за всіма ключами обираємо максимальне значення колізії L_{maxi}.

Крок 8. Розраховуємо середнє арифметичне або центральне значення за максимумами кількостей колізій шляхом знаходження їх математичного очікування $M(L_{maxi})$ (14).

Крок 9. Розраховуємо значення розкиду максимальних значень колізій навколо їхнього центрального значення шляхом знаходження дисперсії ($D(L_{maxi})$) за максимумами кількостей колізій (15).

в) *алгоритм перевірки геш-кодів виконання вимог суворо універсального класу геш-функцій за другим критерієм* полягає у реалізації наступних кроків.

Крок 1. Формуємо два різних випадкових вхідних повідомлення $I_{случ1}$ та $I_{случ2}$.

Крок 2. Формуємо геш-коди $H_{случ1}$ та $H_{случ2}$ для кожного із повідомлень $I_{случ1}$ та $I_{случ2}$.

Крок 3. Формуємо вхідні повідомлення $I_1, I_2, \ldots, I_j \in I$.

Крок 4. Формуємо ключі $K_1, K_2, \ldots, K_j \in K$.

Крок 5. За кожним вхідним повідомленням I_i із застосуванням ключів K_j формуємо їх геш-коди H_{ij}.

Крок 6. Проводимо послідовне порівняння отриманих геш-кодів $H_{случ1}$ та $H_{случ2}$ за однаковим ключем K_j за всіма вхідними повідомленнями із геш-кодами двух випадкових повідомлень: якщо значення геш-кодів співпадають ($H_{ij} = H_{случ1}$ або $H_{ij} = H_{случ2}$), то це свідчить про виникнення колізій (L_j), тоді до лічильника колізій додається 1 (13).

Крок 7. В рамках одного повідомлення за всіма ключами обираємо максимальне значення колізії L_{maxi}.

Крок 8. Розраховуємо середнє арифметичне або центральне значення за максимумами кількостей колізій шляхом знаходження їх математичного очікування значення по максимумам кількості колізій шляхом находження математичного очікування $M(L_{maxi})$ (14).

Крок 9. Розраховуємо значення розкиду максимальних значень колізій навколо їхнього центрального значення шляхом знаходження дисперсії ($D(L_{maxi})$) за максимумами кількостей колізій (15).

Таким чином, виконання даних алгоритмів дозволяє провести оцінку не тільки виконання критеріїв універсальності та суворої універсальності отриманого МАС-коду, а й його рівня стійкості.

3) оцінка практичної реалізації колізійних властивостей геш-кодів.

Додаток, що реалізує пошук колізій у безлічі геш-кодів, сформованих за допомогою модифікованого алгоритму UMAC, розроблено в середовищі об'єктно-орієнтованої мови програмування C#.

З використанням зменшеної моделі UMAC (mini-UMAC) проведемо дослідження колізійних властивостей кодів автентифікації повідомлень, яке полягає в експериментальній оцінці розподілу числа зіткнень (колізій) образів, що формуються. Зменшені моделі покликані дослідити основні показники ефективності криптоалгоритму за збереження його алгебраїчної структури [44].

Оскільки в схемі UMAC (рис. 5) на першому шарі (при формуванні геш-коду) використовуються сімейства універсальних функцій, що гешують, докладно досліджувані в роботах [45-47], статистичні дослідження проведемо тільки на другому шарі при

формуванні псевдовипадкової підложки і на заключному етапі формування кодів (після виконання підсумовування).

Саме на цих етапах, за припущенням авторів [43] і порушуються властивості універсальності формованих кодів автентифікації.

При проведенні статистичних досліджень колізійних властивостей значень геш-кодів, що формуються, для кожного експерименту оцінювалися математичні очікування. $m(n_1)$, $m(n_2)$ та $m(n_3)$, дисперсії $D(n_1)$, $D(n_2)$ та $D(n_3)$, а також для довірчої вірогідності $P_{дов}\left(\left|m(n_i)-m(n_i)\right|<\varepsilon\right)=0,98$ визначається за розрахованими точностями $\varepsilon_1 = t_{kp}\frac{q(n_1)}{\sqrt{n}}$, $\varepsilon_2 = t_{kp}\frac{q(n_2)}{\sqrt{n}}$ та $\varepsilon_3 = t_{kp}\frac{q(n_3)}{\sqrt{n}}$, які відповідають екстремумам довірчих інтервалів (нижнє та верхнє значення виразу) $\left(m(n_i)-\varepsilon; m(n_i)+\varepsilon\right)$. Причому $m(n_i)$ є природною оцінкою для математичного очікування $m(n_i)$ випадкової величини n_i, а $D(n_i)$ – оцінка дисперсії випадкової величини n_i.

Дослідження проводилися над вибіркою, обсяг N = 10 000 елементів. Для формування кожного елемента вибірки розраховувався максимум за множиною M = 1 000 кортежів елементів. Таким чином, загальний обсяг сформованих наборів склав $N \cdot M = 10^7$ елементів. Отримані результати експериментальних досліджень зведено в табл. 1.

Таблиця 1

Результати експериментальних досліджень колізійних властивостей кодів автентифікації, що сформовані з використанням MASH1, MASH2, mini-UMAC MASH1, mini-UMAC MASH2, mini-UMAC AES та mini-UMAC KKK (при Рдов = 0,98)

Статистичні характеристики експерименту	MASH-1	MASH-2	mini-UMAC MASH-1	mini-UMAC MASH-2	mini-UMAC AES	mini-UMAC KKK
$m(n_1)$	***7,09****	***7,14****	1,965	1,968	1,096	1,166
$D(n_1)$	1,69	1,56	0,123	0,120	0,094	0,599
$m(n_1)-\varepsilon_1$	7,061	7,111	1,957	1,961	1,088	1,148
$m(n_1)+\varepsilon_1$	7,122	7,169	1,973	1,977	1,103	1,184
$m(n_2)$	1,013	1,014	*2,629**	*2,64**	1,532	1,161
$D(n_2)$	0,013	0,014	0,349	0,355	0,36	0,67
$m(n_2)-\varepsilon_2$	1,01	1,011	2,62	2,63	1,52	1,14
$m(n_2)+\varepsilon_2$	1,02	1,017	2,64	2,65	1,55	1,18
$m(n_3)$	1,0008	1,0002	**0,237****	**0,224****	**0,0005****	**0****
$D(n_3)$	$9993 \cdot 10^{-8}$	$9999 \cdot 10^{-8}$	0,184	0,177	$499 \cdot 10^{-6}$	0
$m(n_3)-\varepsilon_3$	1,00006	0,9994	0,227	0,214	-2,087	0
$m(n_3)+\varepsilon_3$	1,002	1,0009	0,247	0,234	0,001	0

* – природні оцінки математичних очікувань, якими кількості колізійних значень значною мірою перевищують їх теоретичні оцінки;

** – природні оцінки математичних очікувань, якими кількості колізійних значень не перевищують їх теоретичні оцінки.

Порівняємо отримані результати середньостатистичних оцінок математичних очікувань $m(n_1)$, $m(n_2)$ та $m(n_3)$ кількості правил гешування, за яких виконуються рівності (5), (6) та (7) в [44] відповідно, з теоретичними оцінками: числом $P_{кол} \cdot |H|$ (за першим критерієм), з числом $|H|/|B|$ (за другим критерієм) та числом $P_{кол} \cdot H$ (за третім критерієм).

Розглянемо перший критерій, за яким оцінюється кількість правил гешування, у яких існує колізія (збіг кодів автентифікації) для двох довільних вхідних послідовностей. Відповідно до теоретичних оцінок ця величина обмежена зверху числом $P_{кол} \cdot |H|$. Конкретизуємо цю (теоретичну) оцінку для кодів автентифікації, сформованих з використанням алгоритмів MASH-1, MASH-2, mini-UMAC MASH-1, mini-UMAC MASH-2, mini-UMAC AES та mini-UMAC KKK.

Потужність ключової множини для алгоритмів MASH-1, MASH-2, mini-UMAC MASH-1, mini-UMAC MASH-2, mini-UMAC AES та mini-UMAC KKK дорівнює $|H| = 2^{16}$, потужність безлічі кодів автентифікації, що формуються, також становить $|B| = 2^{16}$. Якщо використовувати верхню оцінку вірогідності колізій як зворотну величину потужності кодів автентифікації, що формуються. $P_{кол} = 2^{-16}$, отримаємо $n_1(x_1,x_2) \le P_{кол} \cdot |H| = 1$ [44].

Колізійні властивості алгоритмів шифрування MASH-1 і MASH-2 суттєво поступаються цій верхній теоретичній оцінці. Фактично, кількість колізій за ними вище за теоретичну межу більш ніж у 7 разів. Коди, сформовані за рештою алгоритмів, також відповідають першому критерію універсальності, оскільки кількість колізій перевищує задану межу. Отже, критерій універсальності не виконується жодним з алгоритмів.

Розглянемо другий критерій, яким оцінюється число правил гешування, у яких для довільної вхідної послідовності значення коду автентифікації не змінюється. Відповідно до теоретичних оцінок ця величина для кодів автентифікації, сформованих з використанням усіх алгоритмів, обмежена зверху числом $|H|/|B| = 1$ [44].

Отримані експериментальні результати свідчать про те, що колізійні властивості кодів авентифікації, сформовані з використанням алгоритмів mini-MASH-1 і mini-MASH-2, не задовольняють другому критерію, оскільки кількість колізій за ними перевищує теоретичну межу майже в 3 рази, а за всіма іншими алгоритмами також спостерігається перевищення допустимої кількості колізій. Отже, перший критерій суворої універсальності також не виконується жодним з алгоритмів, що досліджуються. Відповідно до третього критерію, оцінюється число правил гешування, при яких для двох довільних вхідних послідовностей відповідні їм значення коду автентифікації не змінюються. Теоретична оцінка цієї величини для універсального шешування обмежена зверху числом $P_{кол} \cdot |H|$, що при використанні верхньої оцінки вірогідності колізій $P_{кол} = 2^{-16}$ дає $n_3(x_1,x_2,y_1,y_2) \le P_{кол} \cdot |H| = 1$ [44].

Значення, наведені у табл. 1, свідчать про те, що колізійні властивості кодів аувтентифікації, які сформовані з використанням алгоритмів mini-MASH-1, mini-MASH-2, mini-UMAC AES і mini-UMAC KKK задовольняють другому критерію суворої універсальності. Дані, отримані розрахунковим шляхом, дозволяють стверджувати, що застосування схеми UMAC на KKK значно покращує колізійні властивості кодів контролю цілісності та автентифікації.

4) оцінка ефективності використання модифікованого алгоритму UMAC за розглянутими крипто-кодовими перетвореннями за певними критеріями й умовами, що висуваються.

Для визначення доцільності використання Pad, сформованої за кожним із запропонованих алгоритмів з урахуванням цінності інформації, що захищається, сформуємо комплексний показник ефективності модифікованого алгоритму UMAC (Uкомп):

$$U_{комп} = \left\{ U_{стойк}, U_{опер}, U_{t_{без}} \right\}, \qquad (16)$$

де Uстойк – рівень стійкості криптографічного перетворення [22, 48];
Uопер – рівень оперативності формування криптографічного перетворення [49, 50-52];
Utбез – рівень безпеки за часом [53, 54].

Для оцінки ефективності модифікованого алгоритму UMAC на основі представлених криптоалгоритмів формування псевдовипадкової підложки необхідно використовувати багатофакторний аналіз, оскільки в даному випадку враховується три абсолютно різні фактори (Uстойк, Uопер, Utбез).

Кожен показник може бути розрахований окремо різними методами, а комплексного показника ефективності модифікованого алгоритму UMA методики розрахунку немає. І тут пропонуємо використовувати найпростішу модель багатофакторного аналізу.

Для оцінки комплексного показника ефективності модифікованого алгоритму UMAC було розроблено шкали діапазонів зміни необхідних параметрів із визначенням їх значень як умовних балів. Зокрема, при розробці шкали для Utбез було використано запропоноване в роботі [53] співвідношення необхідного безпечного часу та ступеня секретності інформації. Даний метод оцінки дозволяє отримати досить адекватні результати та поєднати їх з результатами точних розрахунків за окремими параметрами [55, 56]. У табл. 2 наведено шкали оцінки кожного показника.

Таблиця 2

Шкали оцінки рівнів стійкості, оперативності формування і безпеки за часом для псевдовипадкових підложок, сформованих криптоалгоритмами MacElis, MacElis на укорочених та подовжених MEC, а також на збиткових DC, які використовуються в модифікованому алгоритмі UMAC

$U_{стойк}$		$U_{опер}$		$Ut_{без}$	
Бал	*Опис параметру*	*Бал*	*Опис параметру*	*Бал*	*Опис параметру*
1	максимальна потужність (поле Галуа 2^8– 2^{10})	1	повільно	1	низький рівень (від менше ніж 10 хв. до 1 год.)
2	середня потужність (поле Галуа 2^6 – 2^7)	2	середнє	2	допустимо прийнятний рівень (від більше ніж 1 год. до 1 міс.)
3	мінімальна потужність (поле Галуа 2^4 – 2^5)	3	швидко	3	високий рівень (від більше ніж 1 міс. до 1 рік)

Таким чином, на основі багатофакторного аналізу можна описати всі три параметри, які інакше аналітично об'єднати неможливо.

У табл. 3 наведено порівняння криптоалгоритмів формування псевдовипадкової підложки за трьома параметрами.

Використовуючи дані табл. 2, сформуємо таблицю узагальненої ефективності модифікованого алгоритму UMAC за запропонованими криптоалгоритмами формування *Pad* (табл. 4).

Таблиця 3

Порівняння криптоалгоритмів формування псевдовипадкової підложки для модифікованого алгоритму UMAC за показниками Uстойк, Uопер та Utбез

Псевдовипадкова підложка (криптоалгоритми)	Рівень стійкості до криптоперетворень	Рівень оперативності формування конструкції	Рівень безпеки за часом до розшифрування
ННКС MacElis	максимальна потужність (розмірність поля Галуа 2^8–2^{10})	швидко	низький рівень (від менше ніж 10 хв. до 1 год.)
MacElis на укорочених / подовжених МЕС	середня потужність (розмірність поля Галуа 2^6 – 2^7)	середнє	допустимо прийнятний рівень (від більше ніж 1 год. до 1 міс.)
ГККККЗК на МНККС MacElis на укорочених / подовжених МЕС	мінімальна потужність (розмірність поля Галуа 2^4 – 2^5)	повільно	високий рівень (від більше ніж 1 міс. до 1 рік.)

Таблиця 4

Узагальнена оцінка ефективності UMAC за запропонованими криптоалгоритмами формування Pad

Псевдовипадкова підложка (криптоалгоритми)	Умовні бали				Відносна ефективність, %
	Показники			*Узагальнений індекс ефективності*	
	$U_{стойк}$	$U_{опер}$	$Ut_{без}$		
ННКС MacElis (ЕС)	1	3	1	3	15
MacElis на укорочених / подовжених МЕС	2	2	2	8	40
ГККККЗК на МНККС MacElis на укорочених / подовжених МЕС (DC)	3	1	3	9	45
Всього:				20	100

Результати, наведені у табл. 4, представлені у вигляді кругових діаграм (рис. 6, рис. 7), що дозволяють візуалізувати внесок кожного показника в комплексну ефективність модифікованого алгоритму UMAC за запропонованими криптоалгоритмами формування псевдовипадкової підложки.

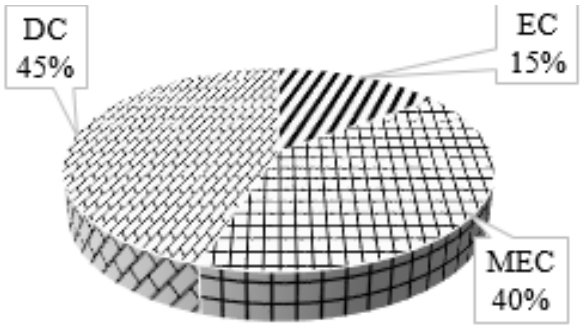

Рис. 6. Комплексний показник ефективності модифікованого алгоритму UMAC за запропонованими криптоалгоритмами формування псевдовипадкової підложки

З табл. 4 та рис. 7 видно, що на сьогодні найкращим криптоалгоритмом для формування псевдовипадкової підложки є той, який використовує підхід завдання збитку (DC).

Також на сьогодні важливим питанням при формуванні ККК є зниження енергетичних витрат (кількість групових операцій) на її формування. На підставі проведених досліджень [49], можна зробити висновок про те, що необхідний рівень стійкості визначає й певні енергетичні витрати на формування псевдовипадкових підложок за досліджуваними криптоалгоритмами (табл. 5). За результатами, представленими в табл. 5 та на рис. 8, можна бачити, що чим вище потужність поля (рівень стійкості), тим більше групових операцій необхідно здійснити, а, отже, вищі енергетичні витрати технічних пристроїв.

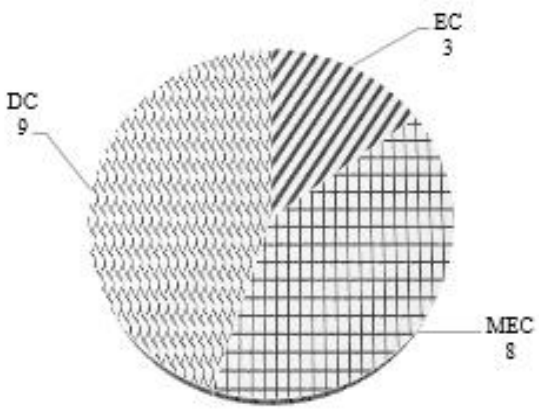

Рис. 7. Нормований показник ефективності модифікованого алгоритму UMAC за запропонованими криптоалгоритмами формування псевдовипадкової підложки

З урахуванням необхідності мінімізувати значення зазначених параметрів для формування ККК, виявлена тенденція є небажаною. Прояв найбільших значень щодо потужності поля та енергетичних витрат продемонстрували ККК, сформовані на класичних ЕС. Тоді як

значення DC на укорочених і подовжених МЕС практично збігаються і, за умови забезпечення однакового рівня стійкості з іншими криптоалгоритмами, споживають найменші енергетичні витрати, а у полі 2^4 демонструють найменші значення своєї групи з різницею у 5,6% на користь укороченого варіанта. Середній рівень значень, що розглядаються ККК, характерний для MacElis на МЕС (подовжених та укорочених), які також дуже близькі між собою (різниця становить 4 % на користь укороченого варіанта).

Таблиця 5

Результати дослідження необхідної кількості групових операцій в різних GF(2^m) [49] при формуванні псевдовипадкової підложки різними криптоалгоритмами

GF(2^m)	НККС MacElis (ЕС)	MacElis на скорочених МЕС	MacElis на подовжених МЕС	ГККК3К на МНККС MacElis на скорочених МЕС (DC)	ГККК3К на МНККС MacElis на подовжених МЕС (DC)
4	–	8293075	8506422	**5612316**	**5942627**
5	10018042	10007947	11156138	7900315	7905257
6	18048068	**17787431**	**18561228**	14892945	14682411
7	32847145	28595014	33210708	25565274	25595014
8	47489784	44079433	48297112	42279183	42116327
9	63215578	61974253	65171690	58963778	58468143
10	**82467897**	79554764	84051337	76564173	75474764

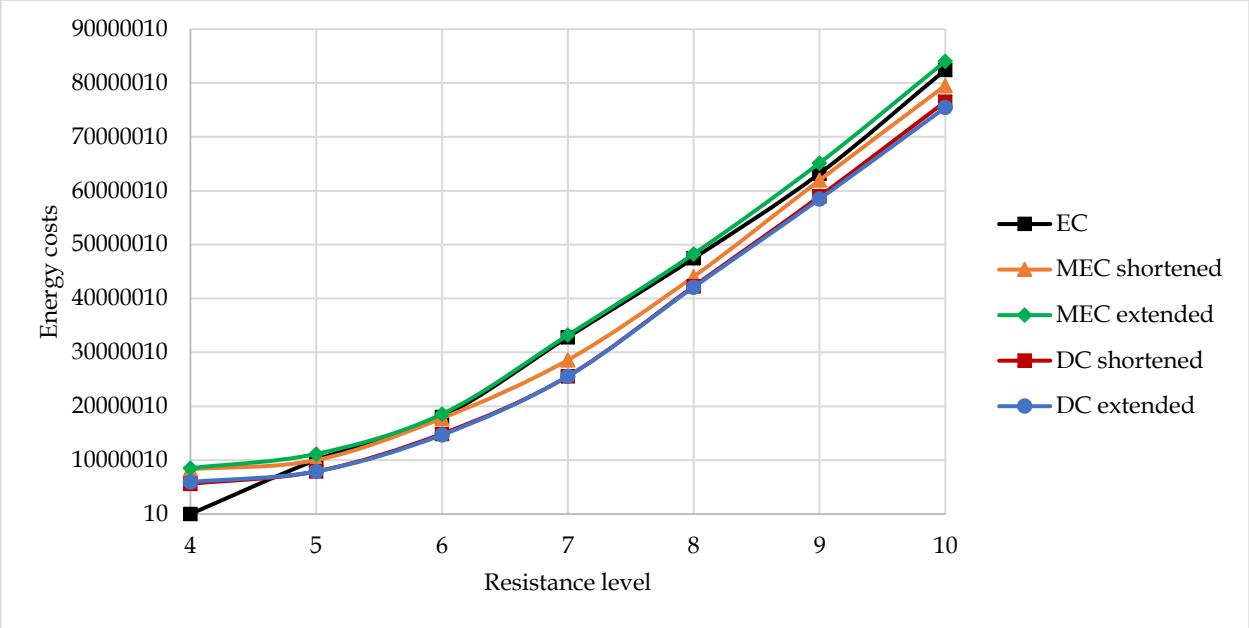

Рис. 8. Залежність змін енергетичних витрат від рівня стійкості криптоалгоритма при формуванні Pad

Висновки. В умовах зростання обчислювальних ресурсів, розширення сфери цифрової економіки, впровадження нових інформаційних технологій у різні сфери професійної діяльності, послуг електронного банкінгу та державного самоврядування, однією з умов забезпечення криптографічної безпеки є пошук різних модифікаційних змін щодо відомих методів.

Зростання та комплексування сучасних загроз, їх гібридність та синергізм вимагають запровадження жорстких критеріїв до спеціальних механізмів забезпечення автентичності. Серед відомих алгоритмів формування МАС-кодів особливу увагу займають універсальні геш-функції. Однак їх застосування без додаткового шифрування геш-коду не забезпечує необхідного рівня стійкості.

Аналіз формування геш-кодів на основі каскадного застосування універсальних геш-функцій показав, що використання механізму псевдовипадкової підложки в алгоритмі UMAC блочного симетричного алгоритму AES не дозволяє забезпечити універсальність геш-коду. А удосконалення механізму на основі модулярної арифметики (алгоритм MASH) не відповідає вимогам з оперативності. Тому було запропоновано використовувати один із перспективних напрямів, який базується на використанні крипто-кодових конструкціях на основі алгеброгеометричних та збиткових кодах.

Модифікаційні зміни було запропоновано ввести до побудови каскадного алгоритму гешування на основі використання крипто-кодових конструкцій на ЕС, МЕС, DC. Це грунтується на тому, що такий підхід

дозволяє підтримувати універсальність і всі переваги даного класу геш-функцій, а також забезпечити необхідні параметри оперативності та стійкості в умовах постквантової криптографії та появи повномасштабного квантового комп'ютера.

Розглянутий алгоритм практичної реалізації методики оцінки критеріїв універсальності та суворої універсальності дозволяє оцінити критерії універсальності та рівень стійкості геш-коду по відношенню до сучасних загроз.

Під час проведення порівняння схем реалізації модифікованого алгоритму UMAC на крипто-кодових конструкціях Мак-Еліса та Нідеррайтера на еліптичних кодах (ЕС), на модифікованих еліптичних кодах (МЕС) та на збиткових кодах (DC), виявлено відмінності щодо формування відкритих ключів та при розшифровуванні повідомлення на стороні одержувача.

Розглянуто фактори, якими необхідно керуватися під час передачі інформації до телекомунікаційних систем. Виділено взаємозв'язок між цінністю інформації та рівнем шкоди від несанкціонованого доступу до неї. Відзначено значний вплив показників рівнів стійкості та оперативності формування псевдовипадкової підложки, а також рівня безпечного часу на її розшифровування.

Проаналізовано оцінку рівня стійкості псевдовипадкової підложки на підставі методик NIST STS 822. В результаті зазначено, що найкращий результат показала псевдовипадкова підложка, сформована на основі збиткових кодів (DC). Отже, найбільш стійкою є псевдовипадкова підложка, сформована на збиткових кодах (DC). На другому місці за стійкістю – на модифікованих еліптичних кодах (МЕС) та на останньому – на традиційних еліптичних кодах (ЕС).

Результати аналізу рівня оперативності формування псевдовипадкової підложки підтвердили те, що крипто-кодові конструкції, сформовані за допомогою криптосистем Нідеррайтера та Мак-Еліса, дозволяють реалізувати криптографічний захист інформації за технологією відкритих ключів та забезпечити швидкість перетворення інформації зі швидкістю шифрування блокових симетричних шифрів.

Аналіз рівня безпечного часу базувався на умови забезпечення необхідного рівня автентифікації псевдовипадкових підложок, сформованих на ЕС, МЕС та DC. Так, для інформації, цінність якої за часом має становити найдовший астрономічний час, рекомендується використовувати криптоалгоритм на DC, а найменший час – на ЕС.

На основі трьох показників розроблено комплексний показник ефективності модифікованого алгоритму UMAC. Значення, отримані при розрахунку узагальненої оцінки ефективності модифікованого алгоритму UMAC за запропонованими криптоалгоритмами формування псевдовипадкових підложок, математично обґрунтували, що найбільш переважним криптоалгоритмом є DC.

У межах дослідження питання зниження енергетичних витрат для формування ККК результати свідчать про те, що найбільших значень щодо потужності поля та енергетичних витрат продемонстрували ККК, сформовані на класичних ЕС. Тоді як значення DC на укорочених і подовжених МЕС практично збігаються і за умови забезпечення однакового рівня стійкості споживають найменші енергетичні витрати.

ЛІТЕРАТУРА

[1] Евсеев, С., Король, О., и Коц, Г. (2015) "Анализ законодательной базы к системе управления информационной безопасностью НСМЭП", Восточно-европейский журнал передовых технологий, вып. 5/3(77), С. 48 – 59. URL: https:// DOI: 10.15587/1729-4061.2015.51468.

[2] Евсеев, С., и Абдулаев, В. (2015) "Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow", Восточно-европейский журнал передовых технологий, вып. 2/2(74), С. 9-15. URL: https: // DOI: 10.15587 / 17294061. 2015.38779.

[3] Актуальные киберугрозы – 2019: тренды и прогнозы (2019), Positive technologies, URL: https: //www.ptsecurity.com.

[4] Актуальные киберугрозы – 2020. Тренды и прогнозы (2020), Positive technologies. URL: https:// www.ptsecurity.com.

[5] Актуальные киберугрозы: итоги 2021 года (2021), Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ cybersecurity-threatscape-2018.

[6] Yevseiev, S., Kots, H., and 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), pp. 11 – 23. URL: https://DOI: 10.15587/1729-4061.2016. 86175.

[7] Yevseiev, S., Korol, O., and Kots, H. (2017) "Construction of hybrid security systems based on the crypto-code structures and flawed codes", Eastern-European Journal of Enterprise Technologies, 4/9(88), pp. 4 – 20. URL: https:// DOI: 10.15587/1729-4061.2016.86175.

[8] Yevseiev, S., and other (2018) "Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes" Eastern-European Journal of Enterprise Technologies, 6/4(96), С. 24-31. URL: https:// DOI: 10.15587/1729-4061.2018.150903.

[9] Guide for Cybersecurity Event Recovery. URL: https://nvlpubs.nist.gov / nistpubs /.../ NIST.SP. 800-184.pdf.

[10] Security requirements for cryptographic modules. URL: https://csrc.nist.gov/publications/fips /fips 140-2/fips1402.pdf.

[11] Guide to LTE Security. URL: https://csrc. nist.gov/publications/drafts/800-187/sp800_187_draft.-pdf.

[12] A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks. URL: https://www.sciencedirect.com/science/article/pii/S2542660520300159.

[13] Hryshchuk, R., Yevseiev, S., & Shmatko, A.(2018) Construction methodology of information security system of banking information in automated banking systems: monograph, Vienna.: Premier Publishing s. r. o., 284 p.

[14] Горбенко, Ю.І., та Ганзя, Р.С. (2014) "Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем",

Східно-Європейський журнал передових технологій, № 1/9 (67), С. 8-16.

[15] Сайт Державної служби спеціального зв'язку та захисту інформації України (2021). "Оперативна інформація Держспецзв'язку щодо захисту державних інформаційних ресурсів" URL: https://cip.gov.ua/ua/news/fakhivci-derzhspeczv-ya zku-z-26-travnya-po-1-chervnya-2021-roku-zablokuvali-44-9-tis-kiberatak-na-derzhavni-informaciini-resursi.

[16] Угрозы кибербезопасности – 2021 (2022) Positive technologies URL: www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2021.

[17] Гаврилова А.А. Анализ состояния блокчейн-проектов на рынке украинских сервисов. Material of International Conference, Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS'2019), 01-02 July. Baku, Azerbaijan, 2019. С. 76.

[18] Regulation (EU) No 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union. Brussels, 2014. pp. 73 – 114.

[19] Bernstein D. J., Buchmann J., Dahmen E. Post-Quantum Cryptography. Berlin-Heidleberg: Springer-Verlag, 2009. URL: doi: http://doi.org /10.1007/978-3-540-88702-7.

[20] Кузнецов А. А., Пушкарев А. И., Сватовский И. И., Шевцов А. В. Несимметричные криптосистемы на алгебраических кодах для постквантового периода. Радиотехника. 2016. № 186, С. 70-90.

[21] Havrylova A. A., Korol O. H., Milevskyi S. V., Bakirova L. R. Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm. Кібербезпека: освіта, наука, техніка. Київ, 2019. № 1(5). pp. 40 – 51.

[22] Горбенко, Ю.І., та Ганзя, Р.С. (2014) "Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем", Східно-Європейський журнал передових технологій, № 1/9 (67), С. 8 – 16.

[23] Сидельников, В.М. (2002) "Криптография и теория кодирования", Материалы конференции "Московский университет и развитие криптографии в России", МГУ, С. 1 – 22.

[24] Yevseev S. P., Rzayev H. N., Korol O. G., Imanova Z. B. Razrabotka modificirovannoy nesimmetrichnoy kripto-kodovoy sistemy Mak-Elisa na ukorochennyh ellipticheskih kodah / S. P. Yevseev, H. N. Rzayev, O. G. Korol, Z. B. Imanova // Vostochno-Yevropeyskiy gurnal peredovyh tehnologiy. – 2016. – № 4/9 (82). – pp. 23-31.

[25] Yevseiev Serhii, Korol Olha, Havrylova Alla. Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece's scheme on elliptical codes / Serhii Yevseiev, Olha Korol Alla Havrylova // Materials of VIIth International Scientific and Technical Conference "Information protection and information systems security": report theses, May 30 –31, 2019. – Lviv: Lviv Polytechnic Publishing House, 2019. – 1 electron. opt. disk (DVD). – С. 86 – 87.

[26] Korol, Olha, Parhuts, Lubomir, & Yevseiev, Serhii (2013) "Metod kaskadnogo preobrazovaniya MAC-kodov s ispolzovaniem modulyarnyh preobrazovaniy" [The method of cascading formation of MAC codes using modular transformations], Nauchnye vedomosti. Seriya Istoriya. Politologiya. Ekonomika. Informatica, № 15 (158), vyp. 27/1, pp. 147 – 157.

[27] Kuznetsov, A.A., Korol, O.H., & Yevseiev, S.P. (2012) "Issledovanie kollizionnyh svoystv kodov autentificatsii soobsheniy UMAC" [Investigation of collision properties of message authentication codes], Prikladnaya radioelectronica: nauch.-tehn. zhurnal. T. 11, № 2, pp. 171–183.

[28] Yevseiev S. P., Iohov O. Y., & Korol O. H. (2013) "Heshuvannia daniih v informaciyniih systemah" [Hashing data in information systems] Monografia. Kharkiv, Ukraiina: Vyd. KhNEU, 213 p.

[29] Kuznetsov, A.A. i dr. (2018) "Porivnjal'ni doslidzhennja ta analiz efektivnosti gibridnoï kodovoï kriptosistemi" [Comparative research and analysis of the efficiency of a hybrid code cryptosystem]. URL: http://nbuv.gov.ua/UJRN/rvmnts_2018_195_9.

[30] "Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography" (2016). IEEE International Symposium in Information. URL: https://DOI:10.1109/ISIT.2016.7541435.

[31] "A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes" (2018), In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018), vol. 2 SECRYPT, pp. 340–347. URL: https://DOI: 10.5330/0006843005060513.

[32] Abidin A. (2012) "On Security of Universal Hash Function Based Multiple Authentication". In: Chim T.W., Yuen T.H. (eds) Information and Communications Security. ICICS 2012. Lecture Notes in Computer Science, vol. 7618. Springer, Berlin, Heidelberg.

[33] Handschuh, H., & Preneel, B. (2008) "Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms". In: Wagner D. (eds) Advances in Cryptology – CRYPTO 2008. CRYPTO 2008. Lecture Notes in Computer Science, vol. 5157. Springer, Berlin, Heidelberg.

[34] "New multicast authentication protocol for entrusted members using advanced encryption standard" URL: https://doi.org/10.1016 /j.ejrs.2011.11.003.

[35] Serhii Yevseiev, Alla Havrylova, Olha Korol, Oleh Dmitriiev, Oleksii Nesmiian [and etc.]. Research of collision properties of the modified UMAC algorithm on crypto-code constructions. "EUREKA: Physics and Engineering". – Tallin: Osauhing "Scientific Route", 2022. – Number 1 (38), pp. 34 – 43.

[36] Olha Korol, Alla Havrylova. Mathematical models of hybrid crypto-code constructions in the UMAC algorithm Przetwarzanie, transmisja i bezpieczenstwo informacji, 2020, Vol. 12. – Bielsko-Biala : Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej. – pp. 125 – 134.

[37] Yevseiev, Serhii, & Havrylova, Alla. Improved UMAC algorithm with crypto-code McEliece's scheme. Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. – Vienna: Premier Publishing s.r.o., 2020.– pp. 79 – 92.

[38] Olha Korol, Alla Havrylova, & Serhii Yevseiev. Practical UMAC algorithms based on crypto code designs. Przetwarzanie, transmisja I bezpieczenstwo informacji, 2019, Tom 2. – Bielsko-Biala: Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej. – pp. 221-232.

[39] Milov, O., Yevseiev, S., Ivanchenko, Y., Tiurin, V., Yarovyi, A. Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 2019, 4(9-100), pp. 6–10.

[40] Gavrilova, A., Volkov, I., Kozhedub, Yu., Korolev R., Lezik, O., Medvediev, V., Milov, O., Tomashevsky, B., Trystan, A., Chekunova, O. (2020). Development of a modified UMAC Algorithm based on crypto-code constructions. Eastern-European Journal of Enterprise Technologies, 4/9 (106), 45 – 63. URL: http://journals.uran.ua/eejet/article/view/210683.

[41] Король, О.Г., Кузнецов, А.А., Евсеев, С.П. (2012). Исследование коллизионных свойств кодов аутентификации сообщений UMAC. Прикладная радиоэлектроника, 2, С. 171–183.

[42] Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems: monograph, Premier Publishing s. r. o., 284. URL: https://www.semanticscholar.org/paper/ CONSTRUCTION-METHODOLOGY-OF-INFORMATION SECURITY-OF-Hryshchuk-Yevseiev/ 7ecb123d60c8cf1941258422d3eb0fb265d9e6fc.

[43] Кузнецов, А.А., Король, О.Г., Босько, В.В. (2011). Модель формирования кодов аутентификации сообщений с использованием универсальных гешерующих функций, Системи обробки інформації, 3(93), С. 117 – 125. URL: http://www. hups.mil.gov.ua/ periodic-app/article/8347.

[44] Евсеев, С.П., Король, О.Г., Огурцов, В.В. (2014). Усовершенствованный алгоритм UMAC на основе модулярных преобразований, Восточно-Европейский журнал передовых технологий, 1/9 (67), С. 16 – 23.

[45] Король, О.Г. (2010). Использование коллизионных свойств кодов аутентификации сообщений UMAC, Системи обробки інформації. Проблеми і перспективи розвитку ІТ-індустрії, 7(88), С. 221-222.

[46] A. Rukhin, and J. Soto, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22", 2000.

[47] Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, and others, "Synergy of building cybersecurity systems": monograph. Kharkiv: PC Technology Center, 2021, 188 p.

[48] А.А. Кузнецов, А.И. Пушкарев, и А.С. Киян, "Алгоритмы электронной цифровой подписи на основе алгебраического кодирования", Радиотехника, Харків, 2017, Вып. 189, С. 59 – 74.

[49] А. Кузнецов, А. Пушкарев, С. Кавун, и В. Калашников, "Несимметричные криптосистемы на основе алгебраического кодирования: современное состояние, существующие противоречия и перспективы практического использования на постквантовый период", Computer science and cybersecurity, Kharkiv : V.N. Karazin Kharkiv National University, 2016, Issue 3(3) 2016, С. 36 – 60.

[50] О.О. Кузнецов, А.І. Пушкарьов, О.В. Шевцов, та Т.Ю. Кузнецова, "Несиметричне криптоперетворення з використанням алгебраїчних блокових кодів", Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф., 23–25 листопада 2016 року, Кропивницький : КНТУ, 2016, С. 124-127.

[51] Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, and Serhii Pohasii, "Socio-Cyber-Physical Systems Security Concept", 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 09-11 June 2022, Ankara, Turkey URL: DOI: 10.1109/HORA55278.2022.9799957.

[52] Serhii Yevseiev, and Alla Havrylova, "Improved UMAC algorithm with crypto-code McEliece's scheme", Modern Problems Of Computer Science And IT-Education: collective monograph. [editorial board K. Melnyk, and O. Shmatko, Vienna: Premier Publishing s.r.o., 2020, pp. 79 – 92.

[53] А. Архипов, "Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации", Науково-технічний журнал "Захист інформації", том 17, №3, С. 211-218, 2015.

[54] С. Евсеев, А. Сочнева, О. Король, и В. Абдулаев, "Анализ методик оценки рисков нарушения безопасности банковской информации", Известия Высших технических учебных заведений Азербайджана. том.19, № 2(106), 2017. – С. 77-86.

УДК 681.3.06

Alla Havrylova, Yuliia Khokhlachova, Volodymyr Pogorelov. Analysis of the application of hybrid crypto-code structures to increase the level of resistance of hash codes to hacking.

Abstract. *The article presents a new way to increase the cryptographic strength of MAC codes for messages transmitted over the Internet. Today, this should make it possible to resist both the consequences of cyber threat aggregation and increase the speed of unauthorized access to data through the creation of such new hardware capabilities as quantum computer technology. The paper proposes to consider the application of the modified UMAC algorithm on modified McEliece elliptic curves using crypto-code structures with hybridity features. The proposed structures were tested for collision properties. For this, a software application was developed in the environment of the object-oriented programming language C#. To determine the capabilities of the studied hash-codes, a complex indicator of the effectiveness of the modified UMAC algorithm was developed. This made it possible to test the proposed designs for resistance to hacking, consider the value of the data that is being protected, and the safe time for a possible hack. As a way to assess this indicator, it was proposed to use the method of multivariate complex analysis. For this, scales for measuring and*

interpreting each indicator were developed. It has been proven that this method of evaluation allows one to obtain adequate results and combine them with the results of accurate calculations for individual parameters. The issue of reducing energy costs for the formation of crypto-code structures was also investigated. The results showed that the creation of hybrid crypto-code structures leads to the lowest energy costs.

***Keywords**: authentication, cryptographic strength, MAC-code, UMAC algorithm, crypto-code constructions, EU, MEC, DC, value of information, safe time.*

Гаврилова Алла Андріївна, старший викладач кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
Alla Gavrilova, senior lecturer of the cyber security department of the National Technical University "Kharkiv Polytechnic Institute".

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Khokhlachova Yuliia, candidate of technical sciences, associate professor of the department of information technology security of the National Aviation University.

Володимир Володимирович Погорелов, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Pogorelov, candidate of Technical Sciences (PhD), Associate Professor of the Information Technology Security department National Aviation University.

Отримано *17 липня 2022 року,* затверджено редколегією *14 листопада 2022 року*