КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.723
УДК 004.056

Корнієць Віктор Анатолійович
Інститут проблем математичних машин і систем
Національної академії наук України, Київ, Україна
ORCID ID: 0000-0002-4967-8395
viktorkorniets@gmail.com

Жданова Юлія Дмитрівна
к.ф.-м.н. доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

МЕТОДИКА ФОРМУВАННЯ ШВИДКІСНОГО ІМІТОСТІЙКОГО ШИФРУ БАГАТО АЛФАВІТНОЇ ЗАМІНИ

Анотація. У статті розглянуто проблеми і задачі формування вимог до побудови швидкісного імітостійкого шифру багато алфавітної заміни на основу принципів функціонування роторних систем, що є актуальним з точки зору забезпечення кіберзахисту об'єктів критичної інфраструктури з підвищеним рівнем ризику порушення сталого функціонування. Проаналізована онтологічна модель сутностей функціональної безпеки автоматизованих систем управління технологічними процесами (АСУ ТП) на об'єктах критичної інфраструктури (ОКІ). Визначено, інструментами підвищення функціональної безпеки у цьому випадку мають бути заходи та засоби кіберзахисту що спрямовані на попередження реалізації загроз перехоплення, аналізу та імітації критичної технологічної інформації та забезпечують корегування обраної політики безпеки. Наголошено, що важливою складовою функціональної безпеки систем та комплексів об'єктів критичної інфраструктури є захист критичної технологічної інформації підчас її передавання каналами зв'язку загального користування. Ефективним механізмом протидії визначеним загрозам є застосування шифру багато алфавітної заміни, для цього запропонована відповідна модель, яка базується на математичних принципах побудови роторних шифрувальних систем, які в рамках моделі позбавлені притаманних їм вразливостей. Модель забезпечує двоетапне перетворення відкритих даних з використанням даних від генератору псевдовипадкової послідовності, в якості якого пропонується модифікована модель алгоритму А5/1, що має необхідні функціональні та криптографічні характеристики. Розглянуті фактори забезпечення криптографічної стійкості запропонованої моделі дозволили обґрунтовано запропонувати швидкісне рішення для обчислення коду автентифікації повідомлення безпосередньо у процесі шифрування.

Ключові слова: кібербезпека, шифрування, криптографія, крипографічний захист, криптоалгоритм, загроза, захист інформації, конфіденційність, цілісність, імітостійкість, об'єкт критичної інфраструктури.

ВСТУП

Повсюдна цифровізація сучасного суспільства створює підґрунтя для нових технологічних проривів, забезпечує вирішення складних завдань в галузі науки та техніки. Швидкість та точність розв'язку задач за допомогою комп'ютерних систем дозволяють збирати та аналізувати великі обсяги інформації від різноманітних сенсорів, майже миттєво вибирати з великої множини рішень раціональний варіант дій виконавчих механізмів та формувати необхідні послідовності керуючих команд. Під

керуючими командами тут і далі розуміється формалізована послідовність символів в певному алфавіті, яка сприймається на приймальній стороні, як доручення виконавчому механізму реалізувати певну дію або забезпечити певний процес.

Фактично, множина команд автоматизованих систем управління виробничими процесами на об'єктах критичної інфраструктури технологічної інформації та даних від сенсорів на керованих пристроях сукупність є критичною технологічною інформацією, яка відповідно до закону віднесена до категорії інформації з обмеженим доступом та підлягає захисту [1].

Слід відмітити, що поєднання інтелектуальних технологій та складних сучасних виробництв може бути потенційно вразливе щодо зловмисних атак, які спрямовані на порушення штатного функціонування певних об'єктів. Майже класичним прикладом подібної атаки став вірус Wi32/Stuxnet, що відомий як перший злоякісний код, який у 2010 році вразив декілька підприємств критичної інфраструктури, а саме: станції зі збагачення урану [2]. Завдяки вірусу Black Energy, який запустив спеціальну програму KillDisk, що не дозволяє завантажуватись комп'ютерам, у 2015 році відбулась атака на обленерго, внаслідок чого 10 районів були повністю знеструмлені [3].

На щастя остання подія не мала катастрофічних наслідків, але ж, зрозуміло, що в умовах повномасштабної війни мають бути підвищені вимоги що забезпечення функціональної безпеки систем та комплексів критичної інфраструктури та уникнення надзвичайних ситуацій, що несуть загрозу здоров'ю та життю людини, та можуть мати катастрофічні наслідки для навколишнього середовища. Такі події, що підвищують ймовірність порушення штатного режиму функціонування системі управління технологічними процесами об'єкта критичної інфраструктури отримали назву інцидентів безпеки критичної інфраструктури.

Загалом, законодавство визначає безпеку критичної інфраструктури як стан її захищеності критичної, за умов якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури [4].

Згідно стандарту ДСТУ EN 61508-1 [5], функціональна безпека (ФБ) є частиною загальної безпеки системи, і, зазвичай, сфокусована на електронному обладнанні та пов'язаному з ним програмному забезпеченні. ФБ націлена на аспекти безпеки, пов'язані з функціонуванням системи або пристрою, і гарантує, що вони працюють правильно у відповідь на команди, які вони отримують. У системному підході ФБ ідентифікує потенційно небезпечні умови, ситуації або події, які можуть призвести до інциденту, за якого може бути завдано шкоди життю та здоров'ю людині або знищено майно. Завдяки цьому вживаються необхідні запобіжних або коригувальні заходи для уникнення або зниження ризику нещасного випадку.

Стандарт встановлює, що дотримання необхідного рівня ФБ систем, комплексів і пристроїв досягається шляхом впровадження алгоритмічних і конструктивних рішень на етапах їх життєвого циклу, а також завдяки реалізації необхідної сукупності організаційно-технічних заходів. При цьому стандарт визначає, що будь-яка стратегія безпеки повинна враховувати не тільки всі елементи, що входять до складу окремих систем (зокрема, сенсори, керуючі пристрої та виконавчі механізми), але також і всі підсистеми безпеки, що входять до складу загальної системи забезпечення безпеки.

Важливою складовою функціональної безпеки систем та комплексів об'єктів критичної інфраструктури є захист критичної технологічної інформації підчас її передавання каналами зв'язку загального користування. Не зважаю на певні напрацювання в цьому напряму це питання досі не зазнало нормативного врегулювання, тому відповідні пошуки ефективних рішень мають бути продовжені.

З урахуванням зазначеного уявляється доцільним проаналізувати цю ситуацію та визначити напрями покращення ефективності безпеки критичної технологічної інформації.

Постановка проблеми. Незважаючи на значну кількість публікацій, що присвячені питанням кібербезпеки інформаційно-комунікаційних технологій та досягнутий на даний час значний прогрес у регулюванні питань захисту критичної інфраструктури та управління ризиками в цій сфері, проблема напрацювання ефективних рішень та формування вимог до захисту критичної технологічної інформації залишається дуже актуальною.

Аналіз останніх досліджень і публікацій. Якщо проаналізувати онтологічну модель сутностей функціональної безпеки автоматизованих систем управління технологічними процесами (АСУ ТП), які функціонують на об'єктах критичної інфраструктури (ОКІ) що можуть мати потенційно небезпечні наслідки у разі втрати контролю за їх функціонуванням (рис. 1).

Наведена на рисунку АСУ ТП здійснює управління певним об'єктом з використанням потенційно вразливого (небезпечного) середовища, яке може бути «прозорим» для системи нападу (джерела загроз), що може здійснювати перехоплення інформаційних потоків, аналізувати поточний стан об'єкта [6] та в режимі реального часу вилучати певні дані, замінювати їх або, навіть формувати хибні послідовності команд, наприклад, шляхом зміни даних, які поступають від сенсорів (виділені на рис. 1 червоним кольором як Дані*).

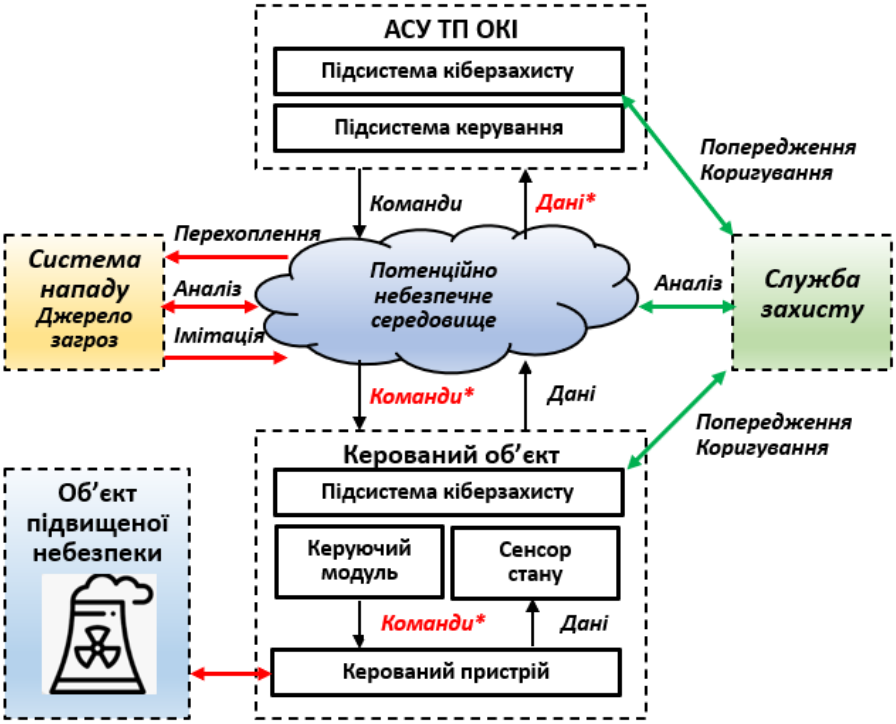

Рис. 1. Онтологічна модель сутностей функціональної безпеки АСУ ТП ОКІ

Хибна послідовність команд (позначені на рис. 1 червоним кольором як Команди*) може спровокувати перехід керованого об'єкту в аварійний стан.

Прикладом потенційно небезпечного середовища можуть бути мережі IoT [7], мережі мобільного доступу [6] та публічні хмари [8].

Інструментами підвищення функціональної безпеки у цьому випадку мають бути заходи та засоби кіберзахисту що спрямовані на попередження реалізації відповідних загроз та забезпечують корегування обраної політики безпеки.

Дієвим механізмом уникнення прозорості мережі інформаційного обміну для зловмисників та підвищення ефективності протидії реалізаціям загроз типу «маскарад» та імітації є методи та засоби криптографічного захисту інформації [9]. У той же час їх створення та провадження повинні враховувати вимоги до умов інформаційного обміну, особливості моделі загроз та моделі вірогідного порушника [10], [11], потребує відповідного дослідження в рамках визначених умов і обмежень.

В [15] вперше для забезпечення гарантоздатності автоматизованих систем управління безпілотними літальними апаратами запропоновано застосування криптосхеми, яка реалізує шифр багатоалфавітної заміни на основі алгоритму генерації підстановок заміни на базі псевдовипадкової послідовності [16]. Криптосхема включає блок контролю (виявлення атак) на модуль криптографічного захисту інформації. В [15] також запропонована оцінка ефективності системи захисту, яка може бути використана для визначення припустимості застосування деяких проектних рішень для побудови системи безпеки. Реалізація багатоалфавітного шифру у цьому випадку підвищує імітостійкість, але не дозволяє контролювати цілісність інформаційних потоків.

Ідея застосування шифру багатоалфавітної заміни набула подальшого розвитку в [13], де запропонована модифікація криптоалгоритму A5/1 для застосування в мережах IoT на пристроях з обмеженими обчислювальними ресурсами. За рахунок запропонованого рішення усунені основні недоліки алгоритму, а саме підвищена стійкість за рахунок збільшення довжину ключа та підвищена імітостійкість, завдяки застосування додаткового секретного параметру — блока підстановок заміни. Рішення оптимізоване до використання на 8-бітних пристроях. Частковим недоліком є фіксоване значення блока заміни.

Метою статті є формування переліку вимог та напрацювання технологічних рішень щодо реалізації криптографічного захисту в АСУ ТП ОКІ з використанням шифру багатоалфавітної заміни з метою підвищення функціональної безпеки технологічного обладнання виробництва за умов дотримання встановлених умов застосування відповідних процедур [12] – [14] в системах нового покоління.

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

Забезпечення функціональної безпеки технологічного обладнання на об’єктах критичної інфраструктури шляхом кіберзахисту відповідних інформаційних технологій завдяки попередженню загроз зловмисного перехоплення, перекручування та нав’язування замість критичної технологічної інформації хибних даних, як було зазначено раніше, може бути реалізовано із застосуванням імітостійкого шифрування на основі шифру багато алфавітної заміни [15]. На рис. 2 зображена умовна схема побудови шифру багато алфавітної заміни.

№ 2 (26), 2024
ISSN 2663 - 4023

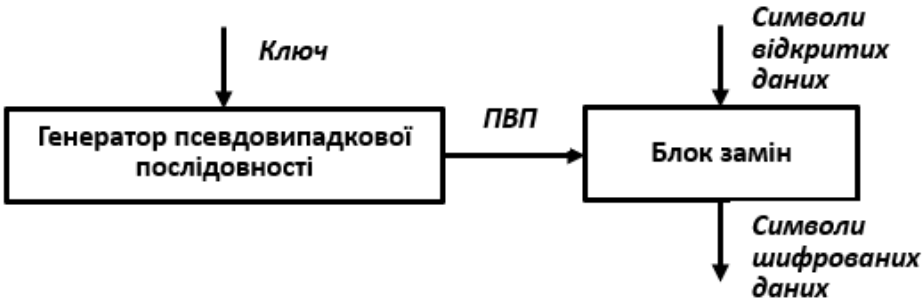

Рис. 2. Схема побудови шифру багато алфавітної заміни

Існує декілька методів побудови шифру багато алфавітної заміни:

- з використанням фіксованої таблиці замін, яка може бути довготерміновим ключем криптосистеми [9], [13];
- на основі підстановки заміни, яка псевдовипадковим чином генерується для зашифрування чергового символу відкритого тексту [16];
- на основі підстановки заміни, що породжується з використанням системи утворюючих елементів та співвідношень [17];
- із застосуванням технології побудови роторних шифрувальних систем [18].

Кожен з перерахованих методів має власні переваги та недоліки.

Використання фіксованої таблиці у випадку відповідної програмної реалізації може забезпечувати вищу швидкість криптоперетворення. Суттєвим недоліком схеми є необхідність поводження з таблицею, як з конфіденційним параметром та передбачувати організаційними заходами її заміну у разі підозри на компрометацію.

Переваги методу псевдовипадкової генерації підстановки заміни проаналізовані в [15], [16]. Основним його недоліком є певна надлишковість процедури, яка зменшує можливу швидкодію шифрування в цьому випадку.

Метод породження підстановок заміни на основі використанням системи утворюючих елементів та співвідношень ефективно реалізується у апаратних засобах криптографічного захисту інформації на основі регістрових схем. Застосування цього методу для програмних реалізації програмних доволі неефективно, оскільки, звичайно, мінімальною одиницею зберігання та обробки інформації в мікропроцесорних системах є байт.

Тривалий час роторні шифрувальні систем були широко застосовані збройними силами різних країн, поступово їх використання практично припинилося. Електромеханічна конструкція таких машин породжувала масу складних проблем, серед яких низька швидкодія, утворення підчас роботи технічних каналів витоку інформації, складність технічного обслуговування, низька надійність, значні масо-габаритні характеристики, несумісність з комп'ютерними технологіями обробки інформації.

Застосування комп'ютерної техніки для реалізації математичних принципів побудови роторних систем дозволяє уникнути перелічених проблем та забезпечити якісно новий рівень імітостійкості шифрування.

Нехай X — підстановка заміни на множині потужності n:

$$X = \begin{pmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1+\delta_1 & 2+\delta_2 & \cdots & n+\delta_n \end{pmatrix} = \begin{pmatrix} i \\ i+\delta_i mod\ n \end{pmatrix}_{i=\overline{1,n}} \quad (1)$$

Тоді позначимо C_μ — шифр Цезаря з параметром μ:

$$C_\mu = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1+\mu & 2+\mu & \cdots & n+\mu \end{pmatrix} = \begin{pmatrix} i \\ i+\mu\ mod\ n \end{pmatrix}_{i=\overline{1,n}}. \quad (2)$$

В загальному випадку рівняння утворення підстановки заміни $Y(\mu)$ в разі реалізації шифрування в системі з одним ротором, що повернутий на μ позицій (умовний кут повороту ротора), має наступний вигляд [18]:

$$Y(\mu) = C_{-\mu} \cdot X \cdot C_\mu. \quad (3)$$

Якщо в роторній системі використовується N роторів $\{X^{(1)}, X^{(2)}, \dots, X^{(N)}\}$, кожен з яких має власний кут повороту, рівняння утворення підстановки заміни набуває наступний вигляд:

$$Y(\mu_1, \mu_2, \dots, \mu_N) = \prod_{j=1}^{N} C_{-\mu_j} \cdot X^{(j)} \cdot C_{\mu_j}. \quad (4)$$

Виходячи із вимог, які впливають на безпеку криптосистем [9], [10], [18], визначимо ряд показників (далі П.1–П.3) що можуть покращити криптографічну стійкість шифрування з використанням підстановок з множини $\{Y(\mu_1, \mu_2, \dots, \mu_N)\}$.

П.1. Бажано забезпечити, щоб кількість різних підстановок заміни у множині $\{Y(\mu_1, \mu_2, \dots, \mu_N)\}$ була максимально наближена до порядку симетричної групи підстановок, а саме: $n!$.

П.2. Вектори параметрів $(\mu_1, \mu_2, \dots, \mu_N)$ рівняння (4) повинні обиратись рівномірно випадковим чином з множини $\{0,1, \dots, n-1\}^N$.

П.3. У підсумку зашифрування будь якого символу відкритого тексту за допомогою навмання вибраної підстановки з множини $\{Y(\mu_1, \mu_2, \dots, \mu_N)\}$ з ймовірністю n^{-1} може бути отриманий будь який символ шифрованого тексту.

Далі, виходячи з форматів подання даних та зручності їх обробки в комп'ютерних системах, а також з урахуванням необхідного об'єму оперативної пам'яті, що необхідна для зберігання даних, уявляється доцільним визначити степінь n підстановок заміни як показникову функцію по основі 2.

Найбільш придатними для обробки на мікроконтролерах, що застосовуються в АСУ ТП, є значеннями $2^4, 2^8, 2^{16}$, які відповідають бітовій довжині даних півбайта, байт та два байти. З урахуванням показника П.1 остаточно визначаємо $n = 2^4$.

Звернемо увагу, що кількість різних підстановок в множині $\{Y(\mu_1, \mu_2, \dots, \mu_N)\}$ вочевидь не перевищує потужності множини векторів $\{(\mu_1, \mu_2, \dots, \mu_N)\}$, яка обчислюється на основі:

$$|\{(\mu_1, \mu_2, \dots, \mu_N)\}| = n^N = 2^{4N}. \quad (5)$$

Використовуючи (5) та на підставі показника П.1 раціонально обрати величину N на основі нерівності:

$$|\{Y(\mu_1, \mu_2, \dots, \mu_N)\}| \leq n^{4N} \leq n!. \quad (6)$$

На основі оцінки Стірлінга для факторіалів:

$$n! \approx \sqrt{2\pi n} \cdot n^n \cdot e^{-n} \quad (7)$$

та з урахуванням нерівності (6) отримуємо оцінку необхідної кількості підстановок заміни у рівнянні (4), а саме: $N \approx 16$.

Таким чином маємо обґрунтування для наступної криптографічної моделі:

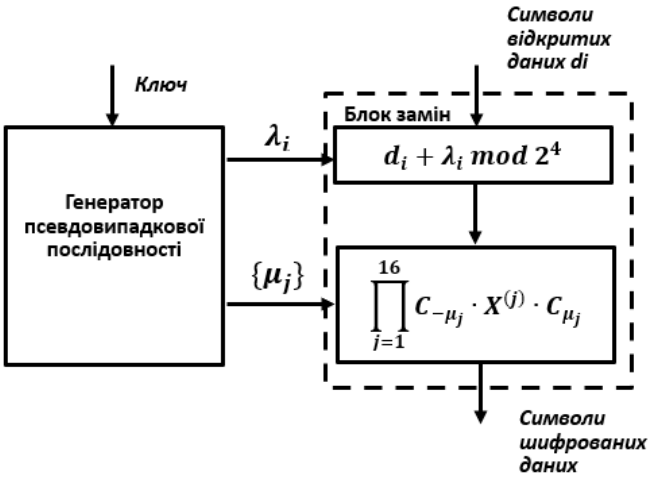

Рис. 3. Модель шифру багатоалфавітної заміни на основі роторних систем

Зображена на рис. 3 модель забезпечує двоетапне перетворення відкритих даних з використанням 68 бітів від генератору псевдовипадкової послідовності, в якості якого пропонується модифікована модель алгоритму A5/1, що має необхідні функціональні та криптографічні характеристики [13].

На першому етапі 4-х бітовий сегмент відкритих даних зазнає перетворення за рівнянням модульного шифрування з використанням рівномірно розподіленого параметру λ_i, що забезпечує рівномірний розподіл модульної суми [19].

Другому етапі за допомогою 16-ті 4-х бітових параметрів $\{\mu_j\}$ отримується 4 зашифрованих рівномірно розподілені біти ξ_i. Це означає, що в разі виконання умови показника П.2 виконується умова показника П.3.

Слід зазначити, що на основі результатів досліджень [20], [21] нескладно показати, що навіть без першого етапу за умов вибору початкових підстановок $\{X_1, X_2, \dots, X_{16}\}$ на другому етапі забезпечується наближення результату шифрування до рівномірного розподілу. Але ж перший етап суттєво знижує вірогідність реалізації атаки на основі відомих відкритого та шифрованого текстів.

Запропонована модель надає можливість швидко формувати код автентифікації повідомлень. Для цього потрібно виконати ще один етап перетворень:

1. Шістнадцять зашифрованих 4 бітних сегмента об'єднаних в 32-бітовий вектор $\Xi = (\xi_i, \xi_{i+1}, \dots, \xi_{i+15})$ зазнають циклічного зсуву вліво на 11 бітів.
2. Результат попереднього кроку за модулем 2^5 додається до суми попередніх значень. Зауважимо, що перше додавання відбувається з константою (*fedcfedc*).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розглянуто проблеми і задачі формування вимог до побудови швидкісного імітостійкого шифру багато алфавітної заміни на основу принципів функціонування роторних систем, що є актуальним з точки зору забезпечення кіберзахисту об'єктів критичної інфраструктури з підвищеним рівнем ризику порушення сталого функціонування.

Розглянуті фактори забезпечення криптографічної стійкості запропонованої моделі дозволили обґрунтовано запропонувати швидкісне рішення для обчислення коду автентифікації повідомлення безпосередньо у процесі шифрування.

Окремим напрямом подальших досліджень, який викликає значний інтерес в плані підвищення ефективності запропонованої системи шифрування, становить задача оцінки швидкості сходження модульних сум випадкових величин на абелевих групах до рівномірного розподілу ймовірностей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On Information, Law of Ukraine №2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Buryachok, V. L. (2013). *Fundamentals of the formation of the state system of cyber security: a monograph.* Kyiv: NAU.
3. *Was there a cyberattack on regional power companies? - BBC News Ukraine.* (2016). BBC News Ukraine. https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.
4. On Critical Infrastructure, Law of Ukraine №1882-IX (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. State Enterprise 'Ukrainian Research and Training Centre for Standardisation, Certification and Quality Problems' (SE 'UkrNDNC') (2019). *Functional safety of electrical, electronic, programmable electronic systems related to safety. Part 1: General requirements (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT)* (DSTU EN 61508-1:2019). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=84383
6. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, E., & Korniets, V. (2022). Vulnerabilities of encryption of short messages in mobile information and communication systems of critical infrastructure. *Electronic professional scientific publication "Cyber Security: Education, Science, Technology", 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
7. Chernenko, R. (2023). Generation of pseudorandom sequences on microcontrollers with limited computing resources, sources of entropy and testing of statistical properties. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 2(22),* 191–203. https://doi.org/10.28925/2663-4023.2023.22.191203
8. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern prospects of applying the Zero Trust concept in building an enterprise information security policy. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
9. Gorbenko, I. D., & Gorbenko, Y. I. (2012). *Applied cryptology: Theory. Practice. Application: monograph.* Kharkiv: FORT.
10. Gorbenko, Y. D. (2015). *Construction and analysis of systems, protocols and means of cryptographic protection of information: monograph.* Kharkiv: FORT.
11. Hulak, H. M., Kashchuk, V. I., & Skladannyi, P. M. (2018). Refined model of the offender and model of cyberattacks implementation in technological process control systems. Actual Problems of State Information Security Management. In: *IX All-Ukrainian Scientific and Practical Conference*, 47–49.
12. Hulak, E. (2024). Methods of rational synthesis of the cryptographic information security subsystem in critical infrastructure networks. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(24),* 282–297. https://doi.org/10.28925/2663-4023.2024.24.282297
13. Korniets, V., & Chernenko, R. (2023). Modification of the cryptographic algorithm A5/1 to ensure the communication of IOT devices. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(20),* 253–271. https://doi.org/10.28925/2663-4023.2023.20.253271
14. Chernenko, R. (2023). Performance evaluation of lightweight cryptography algorithms on limited 8-bit devices. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology, 1(21),* 273–285. https://doi.org/10.28925/2663-4023.2023.21.273285
15. Hulak, H. M., & Skladannyi, P. M. (2017). Ensuring the reliability of automated control and data transmission systems of unmanned aerial vehicles. *Mathematical machines and systems, 3,* 154–161.
16. Hulak, H. M., Buryachok, V. L., & Skladannyi, P. M. (2017) Fast algorithm for generating substitutions of multi-alphabetical substitution. *Information security, 2,* 173–177.
17. Glukhov, M. M., Zubov, A. Y. (1999). On the lengths of symmetric and familiar substitution groups in different systems of formations (review). *Mathematical questions of cybernetics, 8,* 5–32.
18. Konheim, A. G. (1981). *Cryptography: A prime.* Wiley & Sons, Incorporated, New York.
19. Sherstnev, V. I. (1997). Random variable uniformly distributed on a finite abelian group as sum of independent summands Theory Probab. *Appl. Journal, 43(2),* 329–335
20. Berend, D., & Mamana, S. (2021). On random permutations of finite groups. *Journal of Algebraic Combinatorics (2021)54,* 515–528. https://doi.org/10.1007/s10801-020-00999-4
21. Alekseichuk, A. N., & Konyushok, S. N. (2012). *Fourier transform and cryptographic properties of Boolean functions: Tutorial*. K.: ISZI NTUU 'KPI'.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Viktor Korniiets
Institute of Problems of Mathematical Machines and Systems of the
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-4967-8395
viktorkorniets@gmail.com

Yuliia Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

METHODOLOGY FOR FORMING A HIGH-SPEED IMITATOR-RESISTANT CIPHER FOR MULTI-ALPHABET SUBSTITUTION

Abstract. The article considers the problems and tasks of forming requirements for the construction of a high-speed imitation-resistant multi-alphabet substitution cipher based on the principles of rotary systems, which is relevant in terms of ensuring cybersecurity of critical infrastructure facilities with an increased risk of disruption of stable operation. The ontological model of the functional security entities of automated process control systems (APCS) at critical infrastructure facilities (CIF) is analysed. It is determined that the tools for improving functional security in this case should be measures and means of cyber defence aimed at preventing the implementation of threats of interception, analysis and imitation of critical technological information and ensuring the adjustment of the chosen security policy. It is emphasised that an important component of the functional security of systems and complexes of critical infrastructure facilities is the protection of critical technological information during its transmission via public communication channels. An effective mechanism for counteracting these threats is the use of a multi-alphabet substitution cipher, for which purpose a corresponding model is proposed, based on the mathematical principles of constructing rotary encryption systems, which, within the framework of the model, are devoid of their inherent vulnerabilities. The model provides a two-stage transformation of open data using data from a pseudorandom sequence generator, which is a modified model of the A5/1 algorithm that has the necessary functional and cryptographic characteristics. The considered factors of ensuring the cryptographic security of the proposed model allowed us to reasonably propose a high-speed solution for calculating the message authentication code directly in the encryption process.

Keywords: cybersecurity, encryption, cryptography, cryptographic protection, crypto algorithm, threat, information protection, confidentiality, integrity, tamper resistance, critical infrastructure object.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Information, Law of Ukraine №2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Buryachok, V. L. (2013). *Fundamentals of the formation of the state system of cyber security: a monograph.* Kyiv: NAU.
3. *Was there a cyberattack on regional power companies? - BBC News Ukraine.* (2016). BBC News Ukraine. https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.
4. On Critical Infrastructure, Law of Ukraine №1882-IX (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. State Enterprise 'Ukrainian Research and Training Centre for Standardisation, Certification and Quality Problems' (SE 'UkrNDNC') (2019). *Functional safety of electrical, electronic, programmable electronic*

systems related to safety. Part 1: General requirements (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT) (DSTU EN 61508-1:2019). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=84383

6. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, E., & Korniets, V. (2022). Vulnerabilities of encryption of short messages in mobile information and communication systems of critical infrastructure. *Electronic professional scientific publication "Cyber Security: Education, Science, Technology", 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
7. Chernenko, R. (2023). Generation of pseudorandom sequences on microcontrollers with limited computing resources, sources of entropy and testing of statistical properties. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 2(22),* 191–203. https://doi.org/10.28925/2663-4023.2023.22.191203
8. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern prospects of applying the Zero Trust concept in building an enterprise information security policy. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
9. Gorbenko, I. D., & Gorbenko, Y. I. (2012). *Applied cryptology: Theory. Practice. Application: monograph.* Kharkiv: FORT.
10. Gorbenko, Y. D. (2015). *Construction and analysis of systems, protocols and means of cryptographic protection of information: monograph.* Kharkiv: FORT.
11. Hulak, H. M., Kashchuk, V. I., & Skladannyi, P. M. (2018). Refined model of the offender and model of cyberattacks implementation in technological process control systems. Actual Problems of State Information Security Management. In: *IX All-Ukrainian Scientific and Practical Conference*, 47–49.
12. Hulak, E. (2024). Methods of rational synthesis of the cryptographic information security subsystem in critical infrastructure networks. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(24),* 282–297. https://doi.org/10.28925/2663-4023.2024.24.282297
13. Korniets, V., & Chernenko, R. (2023). Modification of the cryptographic algorithm A5/1 to ensure the communication of IOT devices. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(20),* 253–271. https://doi.org/10.28925/2663-4023.2023.20.253271
14. Chernenko, R. (2023). Performance evaluation of lightweight cryptography algorithms on limited 8-bit devices. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology, 1(21),* 273–285. https://doi.org/10.28925/2663-4023.2023.21.273285
15. Hulak, H. M., & Skladannyi, P. M. (2017). Ensuring the reliability of automated control and data transmission systems of unmanned aerial vehicles. *Mathematical machines and systems, 3,* 154–161.
16. Hulak, H. M., Buryachok, V. L., & Skladannyi, P. M. (2017) Fast algorithm for generating substitutions of multi-alphabetical substitution. *Information security, 2,* 173–177.
17. Glukhov, M. M., Zubov, A. Y. (1999). On the lengths of symmetric and familiar substitution groups in different systems of formations (review). *Mathematical questions of cybernetics, 8,* 5–32.
18. Konheim, A. G. (1981). *Cryptography: A prime.* Wiley & Sons, Incorporated, New York.
19. Sherstnev, V. I. (1997). Random variable uniformly distributed on a finite abelian group as sum of independent summands Theory Probab. *Appl. Journal, 43(2),* 329–335
20. Berend, D., & Mamana, S. (2021). On random permutations of finite groups. *Journal of Algebraic Combinatorics (2021)54,* 515–528. https://doi.org/10.1007/s10801-020-00999-4
21. Alekseichuk, A. N., & Konyushok, S. N. (2012). *Fourier transform and cryptographic properties of Boolean functions: Tutorial*. K.: ISZI NTUU 'KPI'.