УДК 004.056.5:65.012.1 DOI: 10.31673/2786-8362.2025.024837

Галаган Н.В., к.т.н.; **Нестеренко К.С.,** д.т.н.;
Волонтир І.В.; Стародубцев Я.О.;
Чумак М.О.

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ СИСТЕМ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ

Halahan N.V., Nesterenko K.S., Volontyr I.V., Starodubtsev Ya.O., Chumak M.O. The problem of ensuring the functional stability of critical infrastructure systems. The article discusses the problems of ensuring the functional resilience of key information management and information and telecommunications systems that belong to critical infrastructure. An analysis of current threats and national and international regulatory approaches is conducted, gaps in the national regulatory and legal framework are identified, and the research problem and objectives are formulated. The main directions of state policy and scientific and technical priorities for improving the resilience of key information infrastructure systems (KII) are presented.

The relevance of the research is determined by the increasing complexity of modern control and communication systems, the deep integration of KII into industrial, energy, transport, and governmental processes, as well as the rising number of cyber incidents with real physical consequences.

It is shown that the main challenges in critical infrastructure are related to cascade effects, where a failure in one component or sector triggers a chain reaction in others. In Ukraine, this problem is aggravated by the lack of unified legal regulation, the absence of a national register of critical systems, inconsistent interagency response procedures, and limited monitoring mechanisms. The paper presents a systematization of key problems in ensuring the resilience of KII, including technical, organizational, and personnel aspects.

The main contribution of this research lies in combining theoretical and applied approaches to enhancing the resilience of critical infrastructure. The developed risk modeling methodology, analytical problem systematization, and proposed policy framework form the basis for an integrated national strategy to improve the reliability and security of Ukraine's critical infrastructure under hybrid threat conditions.

Keywords: functional resilience, critical infrastructure, information security, cascading failures, risk modeling, national security policy

Галаган Н.В., Нестеренко К.С., Волонтир І.В., Стародубцев Я.О., Чумак М.О. Проблема забезпечення функціональної стійкості систем критично важливої інфраструктури. У статті розглянуто проблеми забезпечення функціональної стійкості ключових інформаційно-керуючих та інформаційно-телекомунікаційних систем, що належать до критично важливої інфраструктури. Проведено аналіз сучасних загроз, національних і міжнародних нормативних підходів, виявлено прогалини в національному нормативно-правовому полі, сформульовано постановку задачі та мету дослідження. Наведено основні напрямки державної політики та науково-технічні пріоритети для підвищення стійкості КСІІ (ключових систем інформаційної інфраструктури)

Актуальність теми зумовлена підвищенням складності сучасних інформаційно-керуючих систем, глибокою інтеграцією інформаційно-комунікаційних технологій у промисловість, енергетику, транспорт, державне управління, а також збільшенням кількості кіберінцидентів, що мають фізичні наслідки.

Показано, що ключові виклики у сфері критичної інфраструктури пов'язані з каскадними ефектами, коли порушення роботи одного елемента або сектора спричиняє лавиноподібні відмови в інших. Для України ці процеси ускладнюються відсутністю єдиного нормативно-правового поля, браком державного реєстру КСІІ, неузгодженістю міжвідомчих процедур реагування та обмеженістю механізмів моніторингу технічного стану об'єктів. У роботі здійснено систематизацію проблем у сфері забезпечення стійкості КСІІ, зокрема технічних, організаційних і кадрових. Виявлено, що відсутність єдиних стандартів, слабка сегментація промислових мереж, низький рівень інтеграції систем моніторингу й недосконаліть процедур тестування оновлень формують передумови для системних відмов.

Основний внесок роботи полягає у поєднанні теоретичних і практичних підходів до забезпечення функціональної стійкості критично важливої інфраструктури. Запропонована модель ризиків, аналітична систематизація проблем і комплекс рекомендацій утворюють підґрунтя для формування цілісної національної політики з підвищення надійності та безпеки КСІІ України в умовах гібридних загроз.

Ключові слова: функціональна стійкість, критично важлива інфраструктура, інформаційна безпека, каскадні відмови, моделювання ризиків, національна політика безпеки

© Галаган Н.В., Нестеренко К.С., Волонтир І.В., Стародубцев Я.О., Чумак М.О. 2025

Вступ

Функціональна стійкість систем критично важливої інфраструктури (далі – КСІІ) означає здатність зберігати або оперативно відновлювати критично важливі функції в умовах виникнення випадкових або умисних порушень (кібер-атаки, фізичні впливи, техногенні аварії). У сучасних умовах зростаючої залежності соціально-економічних процесів від інформаційно-комунікаційних технологій та ускладнення архітектур керуючих систем, ризик порушення функціонування таких систем набуває високої критичності. Історичні інциденти (наприклад, Stuxnet або випадки порушення роботи промислового ПЛК після оновлень) демонструють потенціал значних наслідків від втрати функціональності окремих елементів інфраструктури.

Водночас у національному контексті України існують суттєві прогалини: відсутність чітко сформульованих на державному рівні визначень КСІІ, брак національних стандартів та нормативних методик, що ускладнює реалізацію цільової політики з підвищення стійкості відповідних систем.

Аналіз останніх досліджень. Міжнародні підходи до класифікації та захисту КСІІ. У різних країнах сформовано програми інвентаризації критичних об'єктів, розроблено настанови і стандарти (наприклад, ISA/SP99, IEC-профілі для безпечних промислових мереж), а також державні ініціативи з покращення кібербезпеки критичної інфраструктури (у США – Executive Order 13636, PPD-21). Ці підходи поєднують технічні, організаційні та нормативні заходи.

Дослідження в площині моделювання та оцінки ризиків. Окремі наукові праці фокусуються на математичному моделюванні сценаріїв порушень функціонування, системному моделюванні «system-of-systems» для оцінки міжсекторних впливів та побудові симуляцій для підтримки управлінських рішень. Такі підходи дозволяють прогнозувати каскадні ефекти та планувати заходи з підвищення відновлюваності систем.

Практичні кейси та інциденти. Виявлені інциденти останніх років – показові кейси для вивчення механізмів атак та помилок в операційних процесах (комбіновані кібер-фізичні вектори, людський фактор, невдале тестування/поширення оновлень). Аналіз цих подій підкреслює необхідність поєднання кіберзахисту і заходів з фізичної та функціональної безпеки.

Нормативні та організаційні прогалини. Для України відзначають брак національних стандартів і комплексної державної політики щодо КСІІ, що призводить до фрагментарності заходів і розбіжності в підходах у різних галузях/відомствах. Порівняльний аналіз нормативних пакетів США та міжнародних стандартів показує можливі напрямки для адаптації вітчизняних рішень.

Постановка завдання. У даній статті будуть дані ясні визначення і класифікація критично важливих об'єктів та ключових систем інформаційної інфраструктури в контексті України, виходячи з потенційних наслідків порушення їх функціонування. Також буде розглянута розробка методики і механізму національної інвентаризації КСІІ, що враховує міжсекторні залежності й ризики каскадних відмов та сформована модель оцінки актуальних загроз та їхнього впливу на функціональність КСІІ (включно з кібер та комбінованими сценаріями).

Метою роботи є систематизувати загрози й вимоги до функціональної стійкості КСІІ в українському контексті та розробити практично орієнтовані технічні, організаційні та нормативні рекомендації для підвищення стійкості та здатності швидкого відновлення критично важливих систем.

Вклад основного матеріалу дослідження

Перший внесок статті полягає у комплексній систематизації наявних проблем, ризиків і прогалин у забезпеченні функціональної стійкості критично важливих систем інформаційної інфраструктури (КСІІ). Ця систематизація – не просто перелік недоліків, а інструмент для пріоритетизації науково-практичних зусиль, формування дорожніх карт реформ і розробки національних стандартів. Для систематизації використовувався багаторівневий підхід:

Аналіз нормативно-правових актів – збір і порівняння чинних українських документів (у т.ч. законодавчих актів, галузевих положень, наказів органів влади) з міжнародними

практиками й стандартами (ISO/IEC, IEC, ISA). Аналіз виявив розбіжності в термінології, неповне покриття міжсекторних відносин і відсутність уніфікованих процедур інвентаризації.

Огляд наукової і технічної літератури – систематичне опрацювання статей, технічних звітів з метою виявлення типових інцидентів і векторів атак, а також перевірених методик оцінки ризиків. Кейс-аналіз інцидентів – розбір реальних інцидентів (кібер і комбіновані атаки, техногенні аварії) з метою виявлення повторюваних помилок у процедурах управління ризиками та відновлення. На основі зібраних даних сформовано класифікацію проблем за трьома вимірами: технічні, організаційно-правові та кадрово-інституційні.

Технічні проблеми. Нерівномірний рівень впровадження стандартів безпеки в промислових мережах (наприклад, відсутність сегментації, слабке резервування каналів керування, застаріле ПЗ/ПЗП пристроїв). Недостатнє тестування оновлень і відсутність стендів для відтворення виробничих середовищ (відповідальна практика тестування часто відсутня або зведена до формальностей). Низький рівень інтегрованого моніторингу й раннього виявлення аномалій у інфраструктурі.

Організаційно-правові проблеми. Відсутність уніфікованого визначення та реєстру КСІІ на національному рівні; різні органи мають неповні й неконсистентні реєстри. Фрагментарність відповідальності між операторами і державними органами, недостатність механізмів обміну інформацією про інциденти (юридичні, технічні та організаційні бар'єри). Відсутність законодавчо закріплених процедур аудиту, сертифікації та регулярних перевірок готовності критичних систем.

Кадрово-інституційні проблеми. Брак кваліфікованих інженерів із суміжних компетенцій (кіберфізичні системи, промислова безпека, моделювання відмов). Низька інтеграція академічної науки і промисловості: відсутні прикладні програми підготовки, лабораторії для тестування і валідації рішень. Недостатня культура обміну інформацією про інциденти та навчання на помилках.

Наслідки відсутності уніфікованого підходу. Систематизація дозволяє чітко показати, що відсутність уніфікованого підходу призводить до:

- високої імовірності каскадних відмов через непрогнозовані міжсекторні зв'язки;
- затримок у реагуванні та відновленні, коли відповідальність розпорошена між відомствами;
- субоптимальних рішень з інвестицій у безпеку (високі витрати при низькій ефективності заходів).

Результатом є структурований перелік пріоритетів для держави та операторів: визначення та впровадження єдиного реєстру КСІІ, розробка обов'язкових технічних та процедурних стандартів, створення національних тестових лабораторій і програми підготовки кадрів. Ця систематизація також служить основою для побудови методології оцінки ризиків та формулювання державних рекомендацій.

Методологічна база для оцінки ризиків. Запропоновано модель класифікації загроз і сценаріїв каскадних відмов, придатну для використання в процесі національної інвентаризації та планування заходів з підвищення стійкості. Другий ключовий внесок – розробка прикладної методології для кількісної оцінки ризиків, що поєднує локальні характеристики елементів інфраструктури з мережевими ефектами каскадного поширення. Ця методика дає змогу переходити від якісних оцінок до відтворюваних чисельних результатів, що необхідні для планування заходів пом'якшення та оптимізації інвестицій.

Формалізація моделі. Основу методики складає поєднання трьох компонентів:

P_i – ймовірність безпосередньої події (інциденту) для вузла i.

$I_{0,I}$ – локальний вплив/наслідок (економічний, операційний, людський) на скалірованій шкалі.

W_i – коефіцієнт критичності вузла.

Локальний ризик визначається як:

$$R_{local,i} = P_i \cdot I_{0.i} \cdot W_i$$

Мережеве представлення міжсекторних взаємозв'язків:

- Матриця A = $[A_{ij}]$ описує, яку частку впливу порушення вузла j «переносить» на вузол i (нормована так, щоб елементи лежали в інтервалі [0,1]). Важливо: елементи матриці визначаються експертно або на основі статистики інцидентів, а також можуть бути функціями часових параметрів.
- Коефіцієнт α модулює загальну інтенсивність поширення впливу по мережі.

Динамічна модель каскадного поширення. Пропонується лінійна дискретно-часова модель:

$$I(t+1) = \alpha A I(t) + (1-\alpha) I_0$$

де I_0 – вектор первинних локальних впливів. При ρ(αA)<1 маємо стаціонарний розв'язок:

$$I_{ss} = (I - \alpha A)^{-1} I_0$$

Системний вплив I_{ss} відображає стабілізований рівень сукупних наслідків, що включає прямі й опосередковані ефекти.

Побудови та калібрування моделі. Виділяються наступні кроки калібрування моделі:

1. *Збір даних і калькування параметрів* P_i, $I_{0.i}$, W_i – поєднання статистичних даних (інциденти, часи відновлення, збитки) та експертних опитувань; застосування підходів для обробки розріджених даних.

2. *Побудова матриці A* – використання структурних знань (топологія мереж, ланцюги постачання, логістичні залежності) і методів мережевого аналізу; нормалізація та чутливісний аналіз.

3. *Вибір α* – оцінюється через історичні кейси або параметрично (наприклад, шляхом підгонки моделі під відомі каскадні ефекти).

4. *Перевірка умов збіжності* – обчислення спектрального радіуса ρ(αA) і корекція параметрів для забезпечення осмисленості стаціонарного рішення.

5. *Розрахунок сукупного ризику* – введення коефіцієнта β для перетворення системного впливу в одиниці ризику:

$$R_{total,i} = R_{local,i} + \beta \cdot I_{ss,i}$$

6. *Аналіз чутливості й сценаріїв* – варіювання P_i, A, α, β для оцінки найбільш вразливих вузлів і оцінки ефективності заходів.

Приклади математичного застосування. Для невеликих мереж (N ≤ 20) часто достатньо лінійного підходу з точним обчисленням оберненої матриці $(I - \alpha A)^{-1}$. Для більших систем рекомендовано використовувати ітераційні методи (наприклад, метод степеневого розкладу чи ітераційний мультиплікативний підхід) і/або скорочення моделі (агрегація вузлів за доменами).

Валідація й оцінка якості моделі. Перехресна перевірка на історичних інцидентах: модель має вміти відтворити відомі каскади з допустимими похибками. Статистична оцінка невизначеності: присвоєння інтервалів довіри параметрам P_i, A_{ij} і розповсюдження цих невизначеностей у вихідні метрики (через монте-карло симуляції).

Критерії корисності: (1) коректна ідентифікація вузлів, де пом'якшувальні заходи мають найбільший ефект, (2) прогнозування змін R_{total} при впровадженні заходів.

Методологія дає операторам і державним органам кількісний інструмент для пріоритизації інвестицій, планування резервування та оцінки ефективності заходів з підвищення стійкості. Вона дозволяє переходити від інтуїтивних оцінок до відкритих, відтворюваних і перевірюваних рішень.

Практичні рекомендації для державної політики. Сформульовано конкретні напрямки державної політики: удосконалення нормативно-правової бази; створення механізмів моніторингу та реагування; розвиток наукової та промислової політики з метою створення локальних рішень.

Третій внесок – конкретні, практично орієнтовані рекомендації для державної політики й організаційно-правових заходів, що випливають із систематизації проблем і зразкової методології оцінки ризиків. Рекомендації спрямовані на створення регуляторного середовища, яке стимулюватиме підвищення стійкості КСІІ та посилить координацію між суб'єктами.

Ключові блоки політичних ініціатив. *Законодавче закріплення термінології і реєстру КСІІ* – прийняття закону/постанови з чіткими визначеннями: що вважається КСІІ, критерії

віднесення, обов'язки власників і операторів. Створення єдиного державного реєстру критичних об'єктів з доступом для відповідних органів і механізмами захисту конфіденційної інформації.

Нормативно-методичні акти. Розробка й впровадження національних стандартів і методик: інвентаризація, оцінка ризиків, тестування оновлень, планування аварійного відновлення. Обов'язкові процедури регулярних аудитів, валідації заходів безпеки та публічні звіти про готовність.

Система моніторингу та реагування. Створення централізованої або координаційної структури (CSIRT/National CERT для КСІІ) з доступом до агрегованої телеметрії, можливістю проводити координацію реагування та підтримувати оперативний обмін інформацією. Впровадження стандартних процедур обміну інформацією про інциденти (чіткі SLA на оповіщення, формат повідомлень, обмеження відповідальності за розголошення).

Підтримка тестових середовищ і лабораторій. Фінансування й створення національних лабораторій для тестування ПЗ/ОС, моделювання каскадних відмов та відпрацювання сценаріїв реагування. Надання доступу промисловим операторам до ресурсів для тестування оновлень та інтеграцій.

Кадрові ініціативи та науково-освітня політика. Програми підготовки фахівців, курси підвищення кваліфікації, практика стажувань у промислових операторах. Підтримка спільних R&D проектів університетів і промисловості (гранти, спільні лабораторії), стимулювання створення локальних рішень і продуктів.

Рекомендації щодо впровадження та пріоритизації. Пропонуються наступні кроки:

Крок 1 (найближчі 6–12 міс.): визначити базову класифікацію і почати формувати реєстр КСІІ; встановити вимоги до мінімального набору заходів безпеки для операцій критичного рівня.

Крок 2 (1–2 роки): створити центральний координаційний орган для моніторингу; розробити і впровадити стандарти інвентаризації й оцінки ризиків; запустити перші національні лабораторії.

Крок 3 (2–5 років): повна імплементація вимог, обов'язкові аудити, інтегровані системи моніторингу; масове навчання кадрів.

Механізм оцінки ефективності політики. Чіткі KPI: середній час виявлення інциденту (MTTD), середній час відновлення (MTTR), кількість успішних каскадних інцидентів на рік, рівень покриття реєстром. Періодичний аудит політики й корекція на основі аналізу інцидентів і моделювання.

Фінансово-економічні аспекти. Визначення робочих моделей фінансування (державні гранти, приватно-державне партнерство) та економічне обґрунтування інвестицій у лабораторії й підготовку кадрів (оцінка зниження очікуваних збитків після впровадження заходів).

Набір рекомендацій перетворює наукові висновки у конкретну політику: від короткострокових заходів (інвентаризація, мінімальні стандарти) до довгострокових інституційних змін (структури моніторингу, національні лабораторії, освітні програми).

План заходів з підвищення готовності. Перелік кроків для власників КСІІ та державних органів (включно з розробкою стандартів, організацією навчання, створенням реєстру й лабораторій для тестування оновлень та виявлення вразливостей).

Четвертий внесок – практичний план дій для власників КСІІ та державних органів, що деталізує конкретні технічні, організаційні та процедурні кроки для підвищення готовності до інцидентів і скорочення часу відновлення. План побудовано на основі результатів попередніх розділів і методології моделювання ризиків.

Структура плану заходів. План розбитий на три рівні: оперативні (короткострокові), тактичні (середньострокові) та стратегічні (довгострокові) заходи.

Оперативні (0–6 міс.):

- Провести інвентаризацію критичних активів і визначити контактні особи.
- Впровадити базовий набір заходів кібергігієни (патч-менеджмент, сегментація мереж, багатофакторна аутентифікація).

- Підготувати мінімальні аварійні плани (RTO, RPO) для критичних сервісів.
- Налагодити процедуру повідомлення про інциденти і встановити канали оповіщення.

Тактичні (6–24 міс.):

- Впровадити систему централізованого моніторингу телеметрії (SIEM/HDR/OT-monitoring), інтегрувати з національним центром реагування.
- Розгорнути стенди для тестування оновлень і моделювання сценаріїв відмов; проводити регулярні drill/ tabletop exercises.
- Розробити SLA й угоди про обмін інформацією між операторами та державою.
- Розпочати програму навчання та сертифікації інженерів (спільно з університетами).

Стратегічні (2–5 років):

- Створити національні лабораторії та центри компетенції, забезпечити їх обладнанням і персоналом.
- Впровадити механізми фінансового стимулювання для оновлення застарілого обладнання і впровадження резервних рішень.
- Інтегрувати оцінку ризиків у процес прийняття інвестиційних рішень (CAPEX/OPEX) для операторів критичних секторів.
- Формалізувати періодичні перевірки готовності (регуляторні аудити).

Технічні рекомендації. Сегментація і зонування: визначити функціональні зони (контрольна, інженерна, корпоративна) і механізми обмеження перетікання інцидентів між зонами. Резервування критичних каналів: фізичне та логічне дублювання шляхів керування; застосування diverse routing. Автоматичне виявлення аномалій: впровадження алгоритмів машинного навчання для OT/ICS телеметрії з механізмами швидкого відключення і ізоляції. Безпечне оновлення: політики Blue/Green deployment, Canary releases та обов'язкове тестування на стендах.

Організаційні та процедурні кроки. Впровадити план реагування на інциденти (IRP) з чіткими ролями та процедурами. Розробити процедури post-incident review і поширення lessons-learned. Погодити міжоператорські контракти на забезпечення взаємодопомоги в кризових ситуаціях.

Метрики та контроль ефективності. KPI: MTTD, MTTR, кількість успішних відновлень у межах SLA, час на відновлення критичних функцій, частка активів підвищеної готовності. Регулярний аудит відповідності (quarterly/annual), звітування у відповідальні органи.

Верифікація ефективності заходів через модель ризиків. Застосування методології (п.2) до сценаріїв «до/після» впровадження заходів дозволяє кількісно показати зниження R_{total} та скорочення ймовірності каскадних відмов. План включає механізм періодичної адаптації заходів після моделювання і тестування.

Висновки

Підвищення функціональної стійкості систем критично важливої інфраструктури потребує комплексного підходу, що поєднує технічні, організаційні та нормативні заходи. Для України першочерговими кроками мають стати: визначення і законодавче закріплення критеріїв КВО/КСІІ; створення національного реєстру; впровадження єдиних методик оцінки загроз і тестування; формування механізмів моніторингу й реагування; розвиток кадрового та науково-промислового потенціалу. Виконання цих кроків дозволить знизити ймовірність катастрофічних відмов та забезпечити більш швидке відновлення критично важливих функцій у разі інцидентів.

Список використаної літератури:

1. Леоненко Г.П., Юдін А.Ю. Проблеми забезпечення інформаційної безпеки систем критично важливої інформаційної інфраструктури України. // Information Technology and Security, № 1(3), 2013. С. 5–16.

2. Лісецький В.І., Строганов І.В., Чеканов Є.П. Кіберзахист об'єктів критичної інфраструктури: сучасний стан і напрямки розвитку в Україні. // Збірник наукових праць НУОУ, № 4 (53), 2023. С. 45–58.

3. Довгань О.Д., Криворучко О.В. Функціональна стійкість критичних інформаційних систем як об’єкт державного регулювання. // Інформаційна безпека, № 2, 2021. С. 23–32.

4. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. Requirements. International Organization for Standardization, Geneva, 2022.

5. IEC 62443-3-3:2019. Industrial Communication Networks. Network and System Security System Security Requirements and Security Levels. International Electrotechnical Commission, Geneva, 2019.

6. ISA/IEC 62443 Series. Security for Industrial Automation and Control Systems. International Society of Automation, 2018.

7. NIST SP 800-82 Rev.3. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, Gaithersburg, 2023.

8. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. NIST, Gaithersburg, 2012.

Автори статті

Галаган Наталія – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0001-8582-3126

Нестеренко Катерина – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ

ORCID: 0000-0001-7672-7386

Волонтир Ігор – викладач, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0005-1154-9765

Стародубцев Ярослав – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0007-5787-3661

Чумак Михайло – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Authors of the article

Halahan Nataliia – Candidate of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0001-8582-3126

Nesterenko Kateryna – Doctor of Sciences (technical), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0001-7672-7386

Volontyr Ihor – lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0002-6772-1596

Starodubtsev Yaroslav – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0007-5787-3661

Chumak Mykhailo – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.