DOI: 10.18372/2310-5461.54.16757

УДК 004.056:654.026

С. О. Гнатюк, д-р техн. наук, професор
Національний авіаційний університет
orcid.org/0000-0003-4992-0564
e-mail: s.gnatyuk@nau.edu.ua;

В. М. Сидоренко, канд. техн. наук, доцент
Національний авіаційний університет
orcid.org/0000-0002-5910-0837
e-mail: v.sydorenko@ukr.net;

О. Ю. Юдін, канд. техн. наук
Державний науково-дослідний інститут технологій кібербезпеки
orcid.org/0000-0002-4730-1463
e-mail: alex@ukrdeftech.com.ua;

Т. В. Смірнова, канд. техн. наук, доцент
Центральноукраїнський національний технологічний університет
orcid.org/0000-0001-6896-0612
e-mail: sm.tetyana@gmail.com

МЕТОД РОЗРАХУНКУ КРИТИЧНОСТІ ГАЛУЗЕВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Вступ

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем (ІТС), зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки. З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України [1]. Необхідно зазначити, що Законом України «Про основні засади забезпечення кібербезпеки України» [2] визначено необхідність формування переліку об'єктів критичної інфраструктури (ОКІ) та необхідність розробки порядку віднесення об'єктів до ОКІ. Постанова КМУ №1109, про деякі питання ОКІ затверджує:

порядок віднесення об'єктів до ОКІ; Перелік секторів (підсекторів) та основних послуг критичної інфраструктури держави; та Методику категоризації ОКІ [3]. Зазначена Методика описує механізм віднесення ОКІ до певної категорії критичності, який визначається на основі аналізу рівня можливого негативного впливу.

Крім того, нещодавно, набув чинності Закон України Про критичну інфраструктуру [4], який детально описує правові та організаційні засади захисту ОКІ під час створення та функціювання національної системи захисту критичної інфраструктури. Проте не дослідженим досі залишається питання оцінки ефективності захисту ОКІ галузевих ІТС. Водночас, можливо здійснити оцінку ефективності захисту за допомогою механізмів оцінки ризиків.

Тобто, ефективність захисту це зворотна функція від показника оцінки ризику.

Аналіз останніх досліджень та публікацій

Методики оцінки ризиків класифікуються за етапами процесу оцінки ризиків, на яких вони застосовуються [5]: методики ідентифікації ризиків; методики аналізу ризиків — аналіз наслідків; методики аналізу ризиків — якісна, напівкількісна або кількісна оцінка ймовірності; методики аналізу ризиків — оцінка результативності існуючих мір управління; методики аналізу ризиків — кількісна оцінка рівня ризику; методики оцінки ризиків.

Можливість застосування методики для кожного етапу процесу оцінки ризику характеризується наступними рівнями: методика рекомендується до застосування або її можливо застосувати (табл. 1), де РЗ — рекомендований до застосування, МЗ — може бути застосований.

Таблиця 1

Можливість застосування методики для кожного етапу процесу оцінки ризику

Підходи та методики	Процес оцінки ризику				
	Іденти-фікація ризику	Аналіз ризику			Оцінка ризику
		Наслідки	Ймовір-ність	Рівень ризику	
Дослідження небезпеки та працездатності (HAZOP)	РЗ	РЗ	МЗ	МЗ	МЗ
Аналіз сценаріїв	РЗ	РЗ	МЗ	МЗ	МЗ
Аналіз впливу на діяльність	МЗ	РЗ	МЗ	МЗ	МЗ
Аналіз початкової причини	НЗ	РЗ	РЗ	РЗ	РЗ
Аналіз «дерева» несправностей	МЗ	НЗ	РЗ	МЗ	МЗ
Аналіз причини та наслідку	МЗ	РЗ	РЗ	МЗ	МЗ
Аналіз «дерева» рішень	НЗ	РЗ	РЗ	МЗ	МЗ
Аналіз схеми «краватка-метелик»	НЗ	МЗ	РЗ	РЗ	МЗ
Аналіз надійності оператору	РЗ	РЗ	РЗ	РЗ	МЗ
Криві FN	МЗ	РЗ	РЗ	МЗ	РЗ
Показники ризику	МЗ	РЗ	РЗ	МЗ	РЗ
Аналіз витрат та користі	МЗ	РЗ	МЗ	МЗ	МЗ
Багатокритеріальний аналіз рішень (MCDA)	МЗ	РЗ	МЗ	РЗ	МЗ
Матриця наслідків і ймовірності	РЗ	РЗ	РЗ	РЗ	МЗ
Оцінка екологічного ризику (оцінка токсичності)	РЗ	РЗ	РЗ	РЗ	РЗ
Структурована методика «Що, якщо …?» (SWIFT)	РЗ	РЗ	РЗ	РЗ	РЗ
Аналіз характеру та наслідків відмов (FMEA /FMECA)	РЗ	РЗ	РЗ	РЗ	РЗ
Технічне обслуговування, направлене на забезпечення надійності	РЗ	РЗ	РЗ	РЗ	РЗ

Як видно із даних викладених в табл. 1 тільки останні 4 методики є повністю рекомендованими. До факторів, які впливають на вибір методик оцінки ризиків можливо віднести наступні: складність проблеми і методів необхідних для її аналізу; характер та ступінь невизначеності оцінки ризику, який заснований на об'ємі наявної інформації, та тощо, що необхідно для досягнення мети; об'єм необхідних ресурсів в співвідношенні часу та рівня кваліфікації, потреб в даних або затрат; можливість отримання кількісних вихідних даних.

Параметри вибору методик оцінки ризиків розподілені як високий, середній і низький. Найбільш оптимальними, за критеріями можливості отримання кількісних показників, необхідними ресурсами, характером та ступенем невизначеності, а також складністю є методи функціонального аналізу. З урахуванням цього розглянемо ці методи.

Аналіз характеру, наслідків та критичності відмов (FMECA) [6] це методика, що застосовується для визначення того, як відбуваються функціональні відмови компонентів або систем. При цьому, показники критичності, як правило, є якісними або напівкількісними. Водночас, у разі використання фактичних даних інтенсивності відмов, ці показники можуть бути виражені кількісно.

Метод FMECA можна застосовувати для: визначення видів та результатів помилок персоналу; забезпечення процесу планування тестування та технічного обслуговування систем; отримання якісної або кількісної інформації для методик аналізу, таких як аналіз «дерева» несправностей.

До недоліків методу доцільно віднести: застосування для виявлення окремих типів відмов, але не їх поєднань; дослідження можуть потребувати значних затрат часу; застосування для складних систем може бути трудомістким та тривалим.

Технічне обслуговування, спрямоване на забезпечення надійності (RCM) [7] це метод визначення політик, які необхідно проводити для управління відмовами так, щоб ефективно та результативно забезпечити необхідну безпеку, готовність та функціонування всіх типів обладнання.

Метод RCM заснований на оцінці ризику, оскільки цей метод реалізує основні етапи такої оцінки. Тип оцінки ризику – аналіз типів, наслідків та критичності відмов (FMECA).

Ідентифікація ризику спрямована в більшій мірі на ситуації, в яких гіпотетичні відмови можуть усуватись або може знижуватись їх частота та наслідки шляхом виконання завдань по тех-

нічному обслуговуванню. Ідентифікацію ризику виконують шляхом виявлення функцій та стандартів функціонування, а також відмов обладнання та компонентів, що можуть порушувати задані функції.

Аналіз ризику полягає в кількісній оцінці частоти кожної відмови без проведення технічного обслуговування. Наслідки встановлюють шляхом визначення впливу відмови. Матриця ризиків, що поєднує частоту відмови та наслідки, дозволяє встановлювати рівні ризиків. Після цього проводиться оцінювання ризику шляхом вибору відповідної політики управління відмовою для кожного типу відмови.

Методу RCM притаманні ті самі недоліки, що і FMECA.

Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури (ОКІІ), базується на методі FMECA, але за рахунок використання тривимірної матриці критичності, діаграми Парето, причинно-наслідкової діаграми Ісікави та розрахунку додаткових вагових коефіцієнтів критичності дає можливість проводити оцінювання рівня важливості ОКІ [8–11]. До недоліків цього методу необхідно віднести відсутність врахування таких властивостей інформації як, конфіденційність, цілісність, доступність, спостереженість [12].

Метод аналізу критичності на основі ризику запропонований Theocharidou M. базується на аналізі ризиків та може бути застосований до розрахунку кількісних показників захищеності ІТС окремої установи. Зазначений метод не може бути застосований до категорії «держава», тому що він оперує поняттям критичності по відношенню до організації [13–14]. До вад цього методу притаманні недоліки методу визначення рівня важливості ОКІІ.

Проаналізовані методи використовують для визначення критичності механізми оцінки ризиків. Порівняння методів наведено в табл. 2 за такими критеріями: кількість залучених громадян (здоров'я та соціальні наслідки), економічний ефект, політичні наслідки, взаємозалежність секторів критичної інфраструктури (наслідком руйнації одного є руйнація інших), вплив на навколишнє середовище, масштабність за територією, тривалість.

Таблиця 2

Порівняння методів розрахунку критичності ІТС

Назва методу	Ідентифікація ризику	Аналіз			Ідентифікація відмов (за властивостями інформації)	Ідентифікація видів відмов	Можливість отримання кількісних показників	Аналіз критичності
		Наслідки	Імовірність	Рівень ризику				
FMECA	+	+	+	+	–	+	+	–
RCM	+	+	+	+	–	+	+	–
Визначення рівня важливості ОКІІ	+	+	+	+	–	+	+	+
Аналіз критичності на основі ризику	+	+	+	+	–	+	+	+

Постановка проблеми

Проведений аналіз підходів, які можуть використовуватись для оцінки ефективності захисту ІТС показав, що таку оцінку пропонується здійснювати через оцінку ризиків (чим нижчий ризик, тим вище ефективність захисту). У той же час, нормативний документ системи технічного захисту інформації України [15] результатом оцінки визначає рейтинг, який є упорядкованим рядом (переліченням) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Таким чином, виникає протиріччя між підходами до оцінки ефективності захисту. Окрім того, запропоновані методи, які аналізують наслідки, ймовірність настання та рівень ризику, не здійснюють ідентифікацію відмов за властивостями інформації, такими як конфіденційність, цілісність, доступність та спостереженість. На основі встановлених протиріч щодо оцінки ефективності захисту ІТС зроблено висновок про необхідність розробки та практичного використання нових методів оцінки критичності та критеріїв віднесення галузевих ІТС до критичної інфраструктури. Отже, ***метою*** даної статті є розробка та експериментальне дослідження методу розрахунку критичності галузевих ІТС з урахуванням базових властивостей інформації.

Метод розрахунку критичності галузевих ІТС

Метод визначення критичності галузевих ІТС, на відміну від відомих методів [8–11; 13–14], базується на використанні таких властивостей інформації, як конфіденційність, цілісність, досту-

пність, спостереженість, а також враховує кількісні показники критеріїв віднесення до критичної інфраструктури [3; 12; 16]. У загальному випадку метод можна представити у вигляді блок-схеми (рис. 1). Запропонований метод використовує результати структурно-логічної моделі формування функціонального профілю захищеності галузевої ІТС, структурно-функціонального методу формування ФПЗ галузевої ІТС, а також моделі розрахунку кількісного критерію оцінки захищеності ІТС.

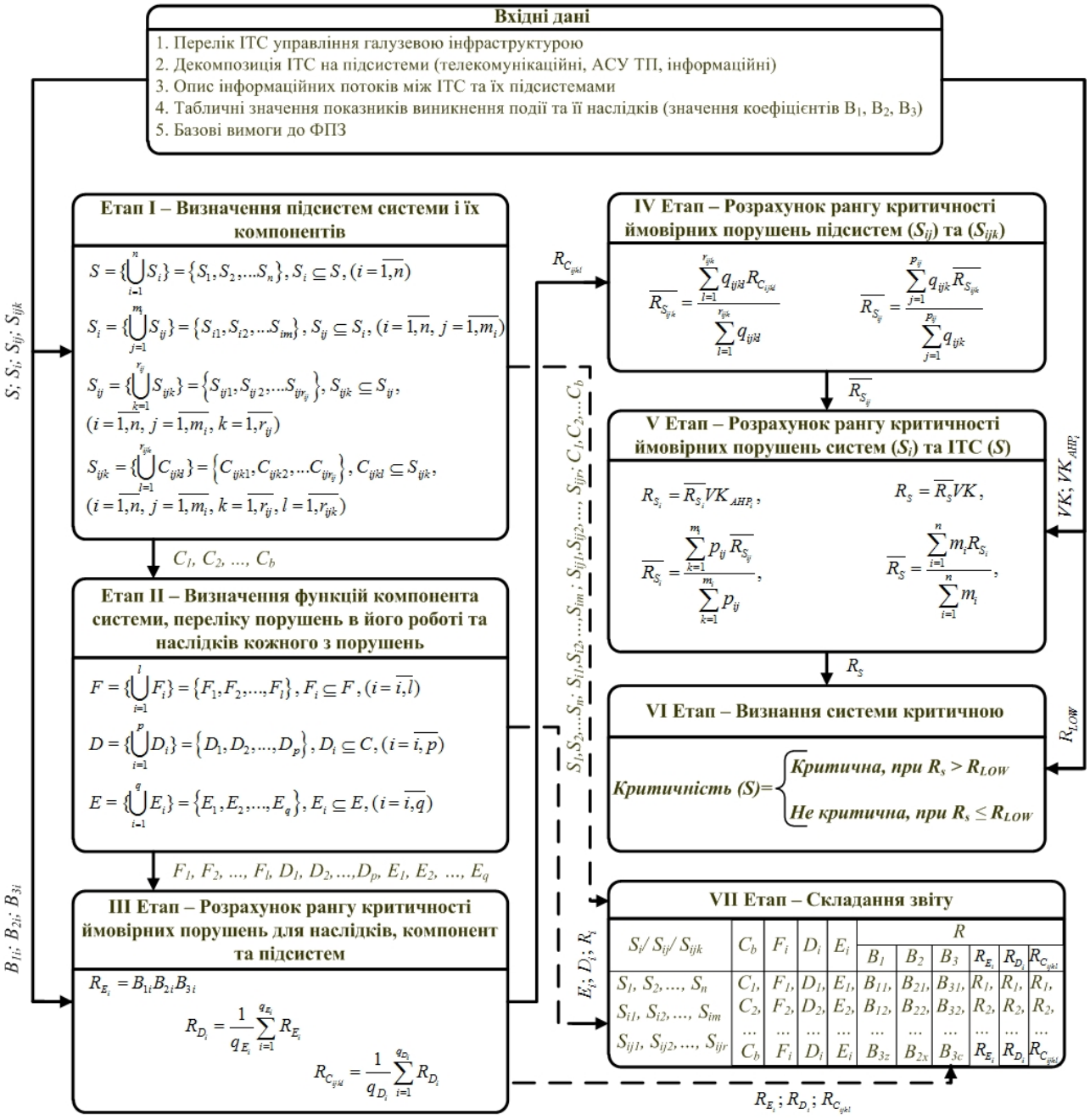

Рис. 1. Блок-схема реалізації методу розрахунку критичності галузевих ІТС

Метод складається з семи етапів, опишемо детально кожен з них.

1. Визначення підсистем ІТС та її компонентів

З метою визначення підсистем ІТС та її компонентів необхідно виконати: 1) декомпозицію інфраструктури галузі на загальні та найбільш критичні домени інфраструктури; 2) декомпозицію критичних доменів на об'єкти; 3) сформувати загальний перелік ІТС; 4) виконати декомпозицію ІТС на підсистеми та компоненти. Перші три пункти описані в роботі [1] та будуть вхідними даними для методу розрахунку критичності.

У загальному випадку, практично всі елементи описані в [1] повинні мати функції кіберзахисту (збереження конфіденційності, цілісності,

доступності, спостереженості, автентичності, неспростовності та достовірності інформації). Зазначені функції можуть бути не основними (наприклад цілісність або доступність інформації в PLC (Programmable Logic Controller) чи оптичних підсилювачах), або основними (антивірусний захист, міжмережевий екран, система охоронної сигналізації, засоби захисту від побічних електромагнітних випромінювань та наведень, засоби криптографічного захисту інформації, засоби автентифікації).

Також необхідно зазначити, що в переліку елементів ІТС управління енергетичною інфраструктурою присутні як засоби, так і системи. Таким чином, доцільно розділяти елементи кіберзахисту ІТС систем управління енергетичною інфраструктурою, на ті, які мають комплекс засобів захисту та ті, що мають комплексну систему захисту інформації [17]. Відповідно до нормативних документів [18] під комплексною системою захисту інформації будемо розуміти сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС, а під комплексом засобів захисту — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації. Додатково зазначимо, що будь-який компонент ІТС, який внаслідок якогонебудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина комплексу засобів захисту [17].

Виходячи з викладеного, до переліку елементів, які забезпечують кіберзахист ІТС систем управління енергетичною інфраструктурою, будемо відносити всі елементи телекомунікаційної підсистеми, автоматизованих систем управління технологічними процесами управління енергетичною інфраструктурою та інформаційні підсистеми. При цьому вимоги, залежно від об'єкту дослідження, будуть висуватись окремо до комплексу засобів захисту та комплексної системи захисту інформації.

Опис елементів ІТС будемо здійснювати у вигляді множин. Склад ІТС ОКІ (S):

$$S = \{\bigcup_{i=1}^{n} S_i\} = \{S_1, S_2, ...S_n\},\ S_i \subseteq S,\ (i = \overline{1,n}), \quad (1)$$

де S_i — клас систем, наприклад: ІТС локального управління виробництвом, ІТС диспетчерського управління і збору даних, а n — загальна кількість класів систем.

Множина систем, що входять до складу ІТС (S_i):

$$S_i = \{\bigcup_{j=1}^{m_i} S_{ij}\} = \{S_{i1}, S_{i2}, ...S_{im}\},\ S_{ij} \subseteq S_i,\ (i = \overline{1,n},\ j = \overline{1,m_i}), \quad (2)$$

де S_{ij} — системи i-го класу, m_i — кількість систем i-го класу, наприклад: АСУ ТП управлінням виробництвом деталей, АСУ ТП ІТС локального управління виробництвом, ІТС диспетчерського управління і збору даних, а n — загальна кількість класів систем.

Множина підсистем для кожної системи ІТС (S_{ij}):

$$S_{ij} = \{\bigcup_{k=1}^{r_{ij}} S_{ijk}\} = \\ = \{S_{ij1}, S_{ij2}, ...S_{ijr_{ij}}\},\ S_{ijk} \subseteq S_{ij},\ (i = \overline{1,n},\ j = \overline{1,m_i},\ k = \overline{1,r_{ij}}), \quad (3)$$

де S_{ijk} — підсистеми S_{ij} систем, r_{ij} — кількість підсистем ij-го класу, наприклад: контрольно-вимірювальні прилади та автоматика, пристрої збору даних з декількох джерел і змінюючих/перетворюючих ці дані в інші формфактори АСУ ТП ІТС локального управління виробництвом.

Множина компонент для кожної підсистеми системи ІТС (S_{ijk}):

$$S_{ijk} = \{\bigcup_{l=1}^{r_{ijk}} C_{ijkl}\} = \{C_{ijk1}, C_{ijk2}, ...C_{ijr_{ij}}\}, \\ = \{C_{ijkl} \subseteq S_{ijk},\ (i = \overline{1,n},\ j = \overline{1,m_i},\ k = \overline{1,r_{ij}},\ l = \overline{1,r_{ijk}}), \quad (4)$$

де C_{ijkl} — компоненти S_{ijk} підсистем, r_{ijk} — кількість компонент ijk-го класу, наприклад: клапани, відсікачі, електричні засувки, датчики тиску, температури, рівню, газоаналізатори, насоси, вакуумвитяжки.

2. Визначення функцій кожного виявленого компонента системи, формування переліку можливих порушень роботи кожного компонента системи, оцінювання наслідків кожного з можливих порушень роботи

Окрім основних функцій компонент системи необхідно враховувати вимоги з безпеки інформації за категоріями логічних інтерфейсів об'єктів доменів. При цьому пропонується використовувати наступні позначення вимог безпеки [19]:

- SG.AC-12 – блокування сесії;
- SG.AC-13 – віддалене переривання сесії;
- SG.AC-14 – дозволені дії без ідентифікації та автентифікації;
- SG.AC-15 – віддалений доступ;
- SG.IA-04 – ідентифікація та автентифікація користувача;
- SG.IA-05 – ідентифікація та автентифікація пристрою;
- SG.IA-06 – автентифікація повідомлень;
- SG.SC-03 – ізоляція функцій безпеки;
- SG.SC-05 – захист від відмови обслуговування;
- SG.SC-06 – пріоритезація ресурсів;
- SG.SC-07 – захист пам'яті;

– SG.SC-08 – цілісність повідомлень (лінії зв'язку);

– SG.SC-09 – конфіденційність повідомлень (лінії зв'язку);

– SG.SC-26 – конфіденційність інформації при зберіганні;

– SG.SI-07 – цілісність програмного забезпечення та інформації.

Функцій кожного виявленого компонента системи (*F*):

$$F = \{\bigcup_{i=1}^{l} F_i\} = \{F_1, F_2, ..., F_l\}, F_i \subseteq F, (i = \overline{i,l}), \quad (5)$$

де F_i — функції компоненти C_{ijkl} підсистеми S_{ijk}; l — загальна кількість функцій компоненти, наприклад: прийняти сигнал, перетворити сигнал, виконати конкретну дію.

Перелік можливих порушень роботи кожного компонента системи (*D*):

$$D = \{\bigcup_{i=1}^{p} D_i\} = \{D_1, D_2, ..., D_p\}, D_i \subseteq C, (i = \overline{i,p}), \quad (6)$$

де D_i — порушення роботи компонента C_{ijkl} підсистем S_{ijk}; p — загальна кількість можливих порушень.

При цьому під порушенням роботи розуміється порушення конфіденційності, цілісності, доступності або спостереженості, які можуть спричинити негативні наслідки.

Наслідки кожного з можливих порушень роботи (*E*):

$$E = \{\bigcup_{i=1}^{q} E_i\} = \{E_1, E_2, ..., E_q\}, E_i \subseteq E, (i = \overline{i,q}), \quad (7)$$

де E_i — наслідки порушень роботи компонента C_{ijkl} підсистем S_{ijk}, q — загальна кількість наслідків.

При цьому під наслідками розуміється відмова в обслуговуванні, розголошення конфіденційних даних, некоректна робота пристроїв.

3. Визначення рангів критичності ймовірних порушень для кожного наслідку порушень та кожного порушення компонента підсистеми

На III етапі визначаються ранги критичності ймовірних порушень (*R*) для кожного наслідку порушень (E_i) та кожного порушення (D_i) компонента C_{ijkl} підсистем S_{ijk}. При визначенні рангів критичності використовуються табличні значення показників [6]. Ранги критичності наслідків порушень E_i роботи компонента C_{ijkl} розраховуються по наступній формулі (R_{E_i}):

$$R_{E_i} = B_{1i} B_{2i} B_{3i}, \quad (8)$$

де B_{1i} — табличне значення показника, що визначає інтенсивність виникнення порушень, B_{2i} — табличне значення показника, що визначає можливість виявлення порушення, B_{3i} — табличне значення показника, що визначає наслідки від виникнення порушення.

Ранги критичності порушення роботи D_i компонента C_{ijkl} розраховуються за формулою (R_{D_i}):

$$R_{D_i} = \frac{1}{q_{E_i}} \sum_{i=1}^{q_{E_i}} R_{E_i}, \quad (9)$$

де R_{E_i} ранг критичності, значення якого відповідає кожному $E_i, (i = \overline{1, q_{E_i}})$, q_{E_i} – кількість наслідків для кожного порушення.

Ранги критичності ймовірних порушень компонент C_{ijkl} підсистеми можна представити у вигляді:

$$R_{C_{ijkl}} = \frac{1}{q_{D_i}} \sum_{i=1}^{q_{D_i}} R_{D_i}, \quad (10)$$

де R_{D_i} ранг критичності, значення якого відповідає кожному $D_i, (i = \overline{1, q_{D_i}})$, q_{D_i} – кількість порушень для кожного компоненту.

4. Обчислення рангів критичності ймовірних порушень підсистем

На IV етапі визначаються ранги критичності ймовірних порушень підсистем S_{ijk} та S_{ij}.

Середнє арифметичне зважене рангу порушення ($\overline{R_{S_{ijk}}}$), для S_{ijk} підсистеми описується наступною формулою:

$$\overline{R_{S_{ijk}}} = \frac{\sum_{l=1}^{r_{ijk}} q_{ijkl} R_{C_{ijkl}}}{\sum_{l=1}^{r_{ijk}} q_{ijkl}}, \quad (11)$$

де $R_{C_{ijkl}}$ – ранг критичності, значення якого відповідає кожному $C_{ijkl}, (l = \overline{1, r_{ijk}})$, q_{ijkl} – кількість порушень для кожного компоненту підсистеми.

Середнє арифметичне зважене рангу порушення ($\overline{R_{S_{ij}}}$) для S_{ij} системи описується наступною формулою:

$$\overline{R_{S_{ij}}} = \frac{\sum_{j=1}^{p_{ij}} q_{ijk} \overline{R_{S_{ijk}}}}{\sum_{j=1}^{p_{ij}} q_{ijk}}, \quad (12)$$

де $\overline{R_{S_{ijk}}}$ – ранг критичності, значення якого відповідає кожній $S_{ijk}, (j = \overline{1, p_{ij}})$, q_{ijk} – кількість порушень для кожної системи.

5. Розрахунок ранків критичності ймовірних порушень систем та ІТС в цілому

На V етапі розраховується ранг критичності ймовірних порушень систем S_i (R_{S_i}) та в цілому ІТС S (R_s).

Ранг критичності систем S_i розраховується по формулі:

$$R_{S_i} = \overline{R_{S_i}} VK_{AHP_i}, \quad (13)$$

де VK_{AHP_i} — коефіцієнт, який характеризує співвідношення заданого ФПЗ до запропонованого експертом в галузі для S_i системи (1), а $\overline{R_{S_i}}$ середнє арифметичне зважене рангу порушення для S_i системи.

VK_{AHP_i} є результатом обчислень за моделлю розрахунку кількісного критерію оцінки захищеності ІТС на основі методу аналізу ієрархій.

$$\overline{R_{S_i}} = \frac{\sum_{k=1}^{m_i} p_{ij} \overline{R_{S_{ij}}}}{\sum_{k=1}^{m_i} p_{ij}}, \quad (14)$$

де $\overline{R_{S_{ij}}}$ — ранг критичності, значення якого відповідає кожній $S_{ij}, (k = \overline{1, m_i})$, p_{ij} — кількість порушень для кожної системи S_{ij}.

Ранг критичності ІТС S (R_S) розраховується за формулою:

$$R_S = \overline{R_S} VK, \quad (15)$$

де VK — коефіцієнт, який характеризує тяжкість наслідків від порушення функціонування ІТС, $\overline{R_S}$ середнє арифметичне зважене рангу порушення для S-об'єкту.

Середнє арифметичне зважене рангу порушення для S-об'єкту розраховується по формулі:

$$\overline{R_S} = \frac{\sum_{i=1}^{n} m_i R_{S_i}}{\sum_{i=1}^{n} m_i}, \quad (16)$$

де $\overline{R_{S_i}}$ — ранг критичності, значення якого відповідає кожному $S_i, (i = \overline{1, n})$, m_i — кількість порушень для кожної системи.

Коефіцієнт тяжкості наслідків від порушення описується формулою:

$$VK = \frac{1}{n} \sum_{j=1}^{m_i} \sum_{i=1}^{n} \frac{VK_{ij}}{VK_{ij}^{\max}}, \quad (17)$$

де $VK_{ij}^{\max}$ — максимальне значення коефіцієнта i-го критерію, який розраховується як добуток пріоритету та найбільшого значення критерію і змінюється від 70 до 10 (табличне значення); n — кількість критеріїв, VK_{ij} — добуток значення i-го та j-го критеріїв.

6. Віднесення ІТС до категорії критичних або некритичних

На VI етапі здійснюється віднесення ІТС (S) до критичних або не критичних:

$$\text{Критичність } (S) = \begin{cases} \text{Критична, при } R_s > R_{low} \\ \text{Не критична, при } R_s \le R_{low} \end{cases}$$

де R_{low} — граничне значення рангу критичності (дорівнює 625,0).

R_{low} є добутком середніх значень VK (5,0), VK_{AHP} (1,0) та $\overline{R_S}$ (125,0).

7. Формування звіту

На VII етапі значення отримані у I–III етапах заносять до звіту, а саме:

- перелік систем, підсистем та їх компонентів;
- перелік функцій компонентів, можливих порушень їх роботи та можливих наслідків;
- значення показників, що визначають інтенсивність виникнення порушень;
- значення показників, що визначають можливість виявлення порушення;
- значення показників, що визначають наслідки від виникнення порушення;
- значення рангів критичності наслідків порушень функції компонента;
- значення рангів критичності наслідків порушень роботи компонента;
- значення рангів критичності порушення роботи компонента;
- значення рангів критичності ймовірних порушень компонент підсистеми.

Зведені відомості викладаються у вигляді табл. 3.

Таблиця 3

Зведені відомості щодо елементів системи

S_i /S_{ij} /S_{ijk}	C_b	F_i	D_i	E_i	R					
					B_1	B_2	B_3	R_{Ei}	R_{Di}	R_{Cijkl}
$S_1, S_2, \ldots, S_n$	C_1	F_1	D_1	E_1	B_{11}	B_{21}	B_{31}	R_1	R_1	R_1
……	…	…	…	…	…	…	…	…	…	…
$S_{ij1}, S_{ij2}, \ldots, S_{ijr}$	C_b	F_i	D_i	E_i	B_{1z}	B_{2x}	B_{3c}	R_{Ei}	R_{Di}	R_{Cijkl}

Експериментальна перевірка методу розрахунку критичності галузевих ІТС

На основі запропонованого у роботі [1] структурно-функціонального методу визначення ФПЗ галузевої ІТС отримано базовий та відкоригований ФПЗ Національної системи конфіденційного зв'язку (НСКЗ):

– FPZB: КА-2, КВ-3, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-2, НП-1;

– FPZE: КА-3, КВ-4, КД-3, КО-1, КК-2, ЦА-4, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-3, ДР-3, НА-1, НИ-2, НК-1, НО-3, НЦ-3, НТ-3, НР-5, НВ-2, НП-1.

FPZE є критерієм оцінки захищеності інформації, що циркулює в НСКЗ. За допомогою методу розрахунку кількісного критерію оцінки захищеності НСКЗ з використанням методу аналізу ієрархій отримане значення $VK_{AHP} = 0,717$. Результат розрахунку VK_{AHP} наведений на рис. 2.

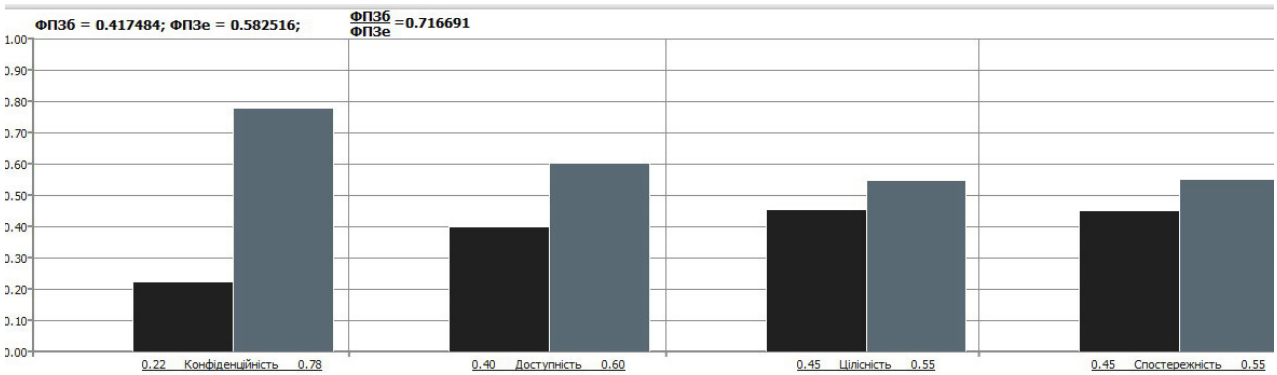

Рис. 2. Результат розрахунків співвідношення альтернатив

Також, виконана декомпозиція НСКЗ на класи систем S_i, множини систем що входять до класів S_{ij}, та їх підсистеми S_{ijk} (табл. 1 в роботі [1]), а також визначені компоненти C_{ijkl}, з яких складається кожна підсистема S_{ijk}.

Фрагмент декомпозиції наведений в табл. 4.

Таблиця 4

Декомпозиція НСКЗ на компоненти

Рівень	Кількість елементів	Позначення системи/підсистеми/компоненту
1	4	S_t, S_s, S_d, S_m
2	10	S_{t1}, S_{t2}, S_{t3}, S_{s1}, S_{s2}, S_{d1}, S_{d2}, S_{d3}, S_{m1}, S_{m2}
3	34	S_{t11}, S_{t12}, S_{t13}, ….., S_{m23}, S_{m24}
4	115	C_{t111}, C_{t112}, C_{t113}, ….., C_{m231}, C_{m241}

Для кожного з компонентів підсистеми визначений перелік функцій F_i, можливих порушень функціонування D_i, наслідків Ei та рангів критичності наслідків R_{Ei}.

Фрагмент переліку функцій наведено в табл. 5.

Таблиця 5

Перелік функцій, можливих порушень, наслідків та рангів критичності

C_i	C_{ijkl}	$ФПЗ$	F_i		D_i		E_i		R_{Ei}	B_{1i}	B_{2i}	B_{3i}
C_{t111}	Телефон	ДС-1, ДВ-1, НТ-2	F_{t1111}	Формування електричного сигналу	D_{t11111}	Відсутність електроживлення	$E_{t111111}$	Відсутність зв'язку	1	1,0	1,0	1,0
							$E_{t111112}$	Неможливість протокол. роботи	5	1,0	5,0	1,0
			F_{t1112}	Аналіз та формування мережевого пакету (ARP, Ethernet, IP…)	D_{t11121}	Пошкодження апаратного забезпечення	$E_{t111211}$	Відсутність зв'язку	1	1,0	1,0	1,0
					D_{t11123}	Некоректні налаштування	$E_{t111231}$	Відсутність зв'язку	2	2,0	1,0	1,0

Використовуючи метод розрахунку критичності галузевих ІТС, здійснений розрахунок рангів критичності R_{D_i} порушення роботи D_i компонента C_{ijkl}, рангів критичності ймовірних порушень $R_{C_{ijkl}}$ компонент C_{ijkl} підсистеми, рангів критичності ймовірних порушень $\overline{R_{S_{ijk}}}$ та $\overline{R_{S_{ij}}}$ підсистем S_{ijk} і S_{ij}, рангів критичності ймовірних порушень R_{S_i} систем S_i та в цілому R_S НСКЗ (S).

Фрагмент результатів розрахунку наведений в табл. 6.

З урахуванням даних наведених в табл. 7 та за (17) зроблений розрахунок коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ $VK = 0,37$.

Таблиця 6

Результати розрахунку рангів критичності

Sijk	*Ci*	*Fi*	*Di*	*Ei*	*Rei*	*Rdijk*	*Rcij*	*Rsijk*	*Rsij*	*Rsi*	*Rs*
S_{t11}	C_{t111}	F_{t1111}	D_{t11111}	$E_{t111111}$	1	3,00	1,87	6,34	13,00	29,95	51,40
				$E_{t111112}$	5						
			D_{t11112}	$E_{t111121}$	1	1,00					
			D_{t11113}	$E_{t111131}$	1	2,33					
				$E_{t111132}$	5						
				$E_{t111133}$	1						
		F_{t1112}	D_{t11121}	$E_{t111211}$	1	1,00					
			D_{t11123}	$E_{t111231}$	2	2,00					
	C_{t113}	F_{t1131}	D_{t11311}	$E_{t113111}$	2	2,00	1,75				
				$E_{t113112}$	2						
			D_{t11312}	$E_{t113121}$	2	1,50					
				$E_{t113122}$	1						
…	…	…	…	…	…	…	…	…	…	…	
S_{m24}	C_{m241}	F_{m2411}	D_{m24113}	E_{m24113}	50	2,00	40	40	40	25,78	

Таблиця 7

Значення показників критеріїв віднесення до критичної інфраструктури

Значення / Критерії	1	2	3	4	5	6	7	8	9	10
Взаємозалежність секторів критичної інфраструктури (наслідком руйнації одного є руйнація інших) (7)		+								
Політичні наслідки (6)				+						
Кількість залучених громадян (здоров'я та соціальні наслідки) (5)	+									
Вплив на навколишнє середовище (4)	+									
Економічний ефект (3)				+						
Масштабність за територією (2)										+
Тривалість (1)				+						

Середнє арифметичне зважене рангу порушення для НСКЗ, що розраховане з виразу (16), становить $\overline{R_S} = 51,40$. За результатами розрахунку (15) отриманий кількісний показник рангу критичності, який дорівнює $R_S = 190,7$, та зроблений висновок, що НСКЗ, на теперішній час, не відноситься до критичних ІТС.

Висновки

У статті було проведено аналіз методів та засобів розрахунку критичності ІТС, який показав, що: оцінка ефективності захисту ІТС здійснюється через оцінку ризиків, що не відповідає вимогам НД ТЗІ; методи оцінки ризику, які аналізують наслідки, ймовірність настання та рівень ризику, не здійснюють ідентифікацію відмов за властивостями інформації (КЦДС); основними критеріями, під час прийняття рішення щодо критичності, є кількість залучених громадян, економічний ефект, політичні наслідки, взаємозалежність секторів критичної інфраструктури, вплив на навколишнє середовище, масштабність за територією, тривалість. Зазначені критерії обов'язково повинні враховуватись при розрахунку критичності галузевих ІТС.

Також у статті представлено удосконалений метод розрахунку критичності галузевих ІТС, який використовує результати структурно-логічної моделі та структурно-функціонального методу формування ФПЗ галузевої ІТС, а також моделі розрахунку кількісного критерію оцінки захищеності ІТС яка базується на використанні методу аналізу ієрархій.

Використання розробленого методу дозволяє здійснити прийняття рішення про віднесення ІТС до категорії критичних з урахуванням властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість.

Крім того, з використанням методу розрахунку критичності галузевих ІТС було проведено

експериментальне дослідження запропонованого методу. Використовуючи даний метод, здійснено розрахунок рангів критичності порушення роботи компонент, підсистем та систем НСКЗ, розрахунок кількісного показника коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ, а також розраховано кількісний показник рангу критичності НСКЗ та, на підставі цього, зроблений висновок щодо критичності НСКЗ.

ЛІТЕРАТУРА

[1] Гнатюк С. О., Юдін О. Ю., Сидоренко В. М., Євченко Я. П. Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем. *Кібербезпека: освіта, наука, техніка*. 2021. Т. 3, № 11. С. 166–182. https://doi.org/10.20998/2522-9052.2021.4.15

[2] Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII. 2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 25.04.2022)

[3] Постанова Кабінету Міністрів України № 1109. 2020. URL: https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n45 (дата звернення 25.04.2022)

[4] Про критичну інфраструктуру, Закон України № 1882-IX. 2021. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення 25.04.2022)

[5] ISO/IEC 31010:2009 – Risk management – Risk assessment techniques, The International Organization for Standardization and The International Electrotechnical Commission. 2009.

[6] IEC 60812 Методы анализа надежности систем. Методы анализа характера и последствий отказа (FMEA).

[7] IEC 60300-3-11 Менеджмент надежности. Часть 3-11: Руководство по применению – Техническое обслуживание, направленное на обеспечение надежности.

[8] Щербак Л. М., Гнатюк С. О., Сидоренко В. М., Шаховал О. А. Метод визначення рівня важливості об’єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Безпека інформації*. 2017. Том 23, №1. С. 27–38. https://doi.org/10.18372/2225-5036.23.11565

[9] Сидоренко В., Гнатюк С., Юдін О. Експериментальне дослідження методу визначення рівня важливості об’єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Захист інформації*, 2017. Том 19, №2. С. 155–172. https://doi.org/10.18372/2410-7840.19.11766

[10] Sydorenko V., Gnatyuk S., Tolbatov A., Fesenko A., Yevchenko Ya., Sotnichenko Yu. Experimental FMECA-based Assessing of the Critical Information Infrastructure Importance in Aviation. CEUR Workshop Proceedings, 2020, Vol. 2732, Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer (ICTERI 2020), October 06-10, 2020, Kharkiv, 2020, P. 136-156.

[11] Gnatyuk S., Sydorenko V., Polihenko O., Sotnichenko Yu., Nechyporuk O. Studies on the Disasters Criticality Assessment in Aviation Information Infrastructure. CEUR Workshop Proceedings, 2020, Vol. 2805, Proceedings of the 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk 2020), October 15–16, 2020, Kherson, 2020, P. 282–296.

[12] Юдін О. Метод визначення критичності галузевих інформаційно-телекомунікаційних систем. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2018. Вип. 1 (35). С. 80–91,

[13] Stergiopoulos G., Kouktzoglou V., Theocharidou M., Gritzalis D. A process-based dependency risk analysis methodology for Critical Infrastructures. *Critical Infrastructures.* 2017. Vol. X, No. Y.

[14] Gritzalis D., Theocharidou M., Stergiopoulos G., Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies, Springer, 2019, 311 p. (Advanced Sciences and Technologies for Security Applications). ISBN 978-3-030-00023-3.

[15] НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, ДСТСЗІ СБ України, 1999.

[16] Звіт про НДР «Дослідження та аналіз проблем захисту інформації на об’єктах критичної інфраструктури», шифр «Інфрастуктура» (д.р. № 0114U000038д).

[17] НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу // ДСТСЗІ СБ України, 1999.

[18] НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу // ДСТСЗІ СБ України, 1999.

[19] National Institute of Standards and Technology Information Report 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, National Institute of Standards and Technology, 2010, 15 p.

Гнатюк С. О., Сидоренко В. М., Юдін О. Ю., Смірнова Т. В.

МЕТОД РОЗРАХУНКУ КРИТИЧНОСТІ ГАЛУЗЕВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем (ІТС), зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки. З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України. Таким чином, виникає необхідність розробки методів та моделей віднесення інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури для забезпечення національної безпеки України. У роботі представлено метод розрахунку рівня критичності галузевих ІТС, що за рахунок використання структурно-логічної та функціональної моделі визначення функціонального профілю захищеності галузевої ІТС, а також функціональної моделі розрахунку кількісного критерію оцінки захищеності ІТС дозволив підвищити точність прийняття рішення про віднесення ІТС до категорії критичних. Використання розробленого методу дозволяє здійснити прийняття рішення про віднесення ІТС до категорії критичних з урахуванням властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість. Крім того, було проведено експериментальне дослідження запропонованого методу на прикладі ІТС Національної системи конфіденційного зв'язку (НСКЗ), за допомогою якого перевірено адекватність реагування методу на зміну вхідних даних. Використовуючи метод розрахунку критичності галузевих ІТС здійснений розрахунок рангів критичності порушення роботи компонент, підсистем та систем НСКЗ, розрахунок кількісного показника коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ, а також розрахований кількісний показник рангу критичності НСКЗ та, на підставі цього, зроблений висновок щодо критичності НСКЗ.

Ключові слова: інформаційно-телекомунікаційні системи (ІТС); критична інфраструктура; об'єкт критичної інфраструктури; критичність; ранг критичності; функціональний профіль захищеності.

Gnatyuk S., Sydorenko V., Yudin O., Smirnova T.

METHOD OF CALCULATING THE CRITICALITY OF SECTORAL INFORMATION AND TELECOMMUNICATION SYSTEMS

Global trends towards an increase in the number and complexity of cyber-attacks led to the actualization of the issue of information and telecommunication systems (ITS) security. In particular, it is important to sectoral ITS, which are critically important for the functioning of society, the socio-economic development of the state and ensuring the informational component of national security. Taking into account the needs of national security and the need to introduce a systemic approach for solving the problem of critical infrastructure protection, at the national level, creating a security system is one of the priorities in the reforming of the defense and security sector of Ukraine. Thus, there is a need to develop methods and models for the ITS categorization as critical information infrastructure to ensure the national security of Ukraine. The paper presents a method for calculating the level of criticality of sectoral ITS, which, due to the use of a structural-logical and functional model for determining the functional profile of the sectoral ITS security, as well as a functional model for calculating the quantitative criterion for assessing the security of ITS, allow to increase the accuracy of the decision to categorize ITS as critical. The use of the developed method makes it possible to make a decision to categorize ITS as critical, taking into account the properties of information (such as confidentiality, integrity, availability, observability). In addition, an experimental study of the proposed method was carried out on the example of the ITS of the National Confidential Communication System (NCCS), which was used to check the adequacy of the method's response to changes in input data. Using the method of calculating the criticality of sectoral ITS, the calculation of the criticality ranks for the functionality disruption of components, subsystems and systems of NCCS was carried out; the calculation of the quantitative indicator of the severity of the consequences of the functionality disruption of NCCS, as well as the quantitative indicator of the rank of criticality of NCCS was calculated and a conclusion was made regarding the NCCS criticality.

Keywords: information and telecommunication systems (ITS); critical infrastructure; critical infrastructure object; criticality; criticality rank; functional security profile.

Стаття надійшла до редакції 24.05.2022 р.
Прийнято до друку 15.06.2022 р.