Наукові перспективи
Видавнича група

Наука і Техніка Сьогодні

№ 4 (58)
2026

З Україною в серці!

Видавнича група «Наукові перспективи»

Всеукраїнська Асамблея докторів наук із державного управління

«Наука і техніка сьогодні»

Випуск № 4(58) 2026

Київ – 2026

Publishing Group «Scientific Perspectives»

Ukrainian Assembly of Doctors of Sciences in Public Administration

"Science and technology today"

Issue № 4(58) 2026

Kyiv – 2026

ISSN 2786-6025 Online

УДК 001.32:1 /3](477)(02)

R40-05553

DOI: **https://doi.org/10.52058/2786-6025-2026-4(58)**

«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)»: журнал. 2026. № 4(58) 2026. С. 5059

Згідно наказу Міністерства освіти і науки України від 07.04.2022 № 320 журналу присвоєно категорію "Б" із економіки та педагогіки (спеціальності – 015 - Педагогічні науки; 076 - Економічні науки)

Згідно наказу Міністерства освіти і науки України від 06.06.2022 № 530 журналу присвоєно категорію "Б" із права (спеціальність – 081 Юридичні науки)

Згідно наказу Міністерства освіти і науки України від 10.10.2022 № 894 журналу присвоєно категорію "Б" із техніки (спеціальність - 122 Комп'ютерні науки)

Журнал видається за підтримки Міждержавної гільдії інженерів консультантів, Інституту філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан), громадської організації «Християнська академія педагогічних наук України» та громадської організації «Всеукраїнська асоціація педагогів і психологів з духовно-морального виховання»

Рекомендовано до видавництва Президією Всеукраїнської Асамблеї докторів наук з державного управління (Рішення від 24.04.2026, № 8/4-26)

Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), міжнародної пошукової системи Google Scholar та до міжнародної наукометричної бази даних Research Bible

Згідно Порядку формування Переліку наукових фахових видань України, затвердженого наказом МОН України від 15.01.2018 № 32, повнотекстовий доступ до наукових статей журналу представлений на платформі «Наукова періодика України» в Національній бібліотеці України імені В.І. Вернадського НАН України та в Національному репозитарії академічних текстів

ISSN 2786-6025 Online

№ 4(58) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.056:624.19
https://doi.org/10.52058/2786-6025-2026-4(58)-3844-3855

Любинський Петро Леонідович аспірант, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, https://orcid.org/0009-0004-3471-2206

Почанський Олег Михайлович кандидат технічних наук, викладач, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, https://orcid.org/0009-0006-6093-2987

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ СТІЙКОСТІ ОБ'ЄКТІВ ПІДЗЕМНИХ ІНЖЕНЕРНИХ МЕРЕЖ

Анотація. У статті досліджено особливості забезпечення інформаційної стійкості об'єктів підземних інженерних мереж як складової критично значущої інфраструктури. Обґрунтовано, що в умовах стрімкої цифровізації та зростання кількості кіберзагроз підземні мережі, зокрема системи водопостачання, газопроводи, теплотраси, електромережі та телекомунікаційні кабелі, стають вразливими не лише до фізичних пошкоджень, але й до інформаційних та кібернетичних впливів. Визначено, що інформаційна стійкість таких систем полягає у здатності забезпечувати безперервність функціонування, цілісність і достовірність даних, ефективне реагування на інциденти, а також швидке відновлення після порушень.

Розглянуто основні складові інформаційної стійкості, зокрема запобігання загрозам, своєчасне виявлення відхилень, адаптацію до змін середовища та відновлення працездатності систем. Проаналізовано сучасні підходи до забезпечення стійкості, що базуються на інтеграції технічних засобів захисту (SCADA-системи, IoT-платформи, системи виявлення вторгнень, резервування та шифрування), організаційних заходів (політики безпеки, управління ризиками, навчання персоналу) та аналітичних інструментів (моніторинг у реальному часі, прогнозування аварій, аналіз аномалій).

Особливу увагу приділено специфіці підземних інженерних мереж, які характеризуються значною територіальною розподіленістю, складністю доступу та високою залежністю від безперервності функціонування. Наведено приклади сучасних технологій і систем моніторингу, що дозволяють підвищити рівень інформаційної стійкості та мінімізувати наслідки аварій і кібератак.

Зроблено висновок, що забезпечення інформаційної стійкості підземних мереж є складним міждисциплінарним завданням, яке потребує комплексного

ISSN 2786-6025 Online

підходу, впровадження міжнародних стандартів та подальших наукових досліджень у сфері кібербезпеки та управління критичною інфраструктурою.

Ключові слова: інформаційна стійкість, критична інфраструктура, підземні інженерні мережі, SCADA, кібербезпека, моніторинг, IoT.

Liubynskyi Petro Leonidovych Postgraduate Student, Simon Kuznets Kharkiv National University of Economics, Kharkiv, https://orcid.org/0009-0004-3471-2206

Pochanskiy Oleh Mykhailovych PhD in Technical Sciences, Lecturer, Simon Kuznets Kharkiv National University of Economics, Kharkiv, https://orcid.org/0009-0006-6093-2987

FEATURES OF INFORMATION RESILIENCE OF UNDERGROUND ENGINEERING NETWORK FACILITIES

Abstract. The article examines the features of ensuring the information resilience of underground engineering network facilities as a component of critical infrastructure. It is substantiated that under conditions of rapid digitalization and the growing number of cyber threats, underground networks – such as water supply systems, gas pipelines, heating networks, power grids, and telecommunication cables – are becoming vulnerable not only to physical damage but also to informational and cyber impacts. It is determined that the information resilience of such systems lies in their ability to ensure continuity of operation, integrity and reliability of data, effective incident response, and rapid recovery after disruptions.

The main components of information resilience are considered, including threat prevention, timely detection of anomalies, adaptation to environmental changes, and system recovery.

Modern approaches to resilience assurance are analyzed, based on the integration of technical protection means (SCADA systems, IoT platforms, intrusion detection systems, redundancy, and encryption), organizational measures (security policies, risk management, personnel training), and analytical tools (real-time monitoring, failure prediction, anomaly detection).

Special attention is paid to the specifics of underground engineering networks, which are characterized by significant spatial distribution, limited accessibility, and a high dependence on continuous operation. Examples of modern technologies and monitoring systems that enhance information resilience and minimize the consequences of accidents and cyberattacks are provided.

It is concluded that ensuring the information resilience of underground networks is a complex interdisciplinary task that requires a comprehensive approach,

ISSN 2786-6025 Online

implementation of international standards, and further research in the field of cybersecurity and critical infrastructure management.

Keywords: information resilience, critical infrastructure, underground engineering networks, SCADA, cybersecurity, monitoring, IoT.

Постановка проблеми. Сучасні підземні інженерні мережі є невід'ємною складовою критично значущої інфраструктури, від стабільності функціонування якої залежить життєдіяльність міст, економічна безпека та соціальна стабільність. Активна цифровізація цих систем, впровадження SCADA та IoT-технологій значно підвищують ефективність управління, але водночас створюють нові вектори загроз, зокрема кібернетичних.

Традиційні підходи до безпеки, орієнтовані переважно на захист від окремих загроз, не забезпечують належного рівня стійкості в умовах комплексних ризиків, що поєднують фізичні, техногенні та кібернетичні впливи. Це зумовлює необхідність переходу до концепції інформаційної стійкості, яка враховує здатність системи не лише протистояти загрозам, але й адаптуватися, функціонувати в умовах інцидентів та швидко відновлюватися.

Отже, актуальним є дослідження особливостей забезпечення інформаційної стійкості підземних інженерних мереж та визначення ефективних підходів до її підвищення.

Аналіз останніх досліджень і публікацій. Питання інформаційної стійкості активно досліджується у сучасній науковій літературі в контексті кібербезпеки та захисту критичної інфраструктури. Більшість досліджень розглядає стійкість як розширення традиційної інформаційної безпеки, що включає здатність до адаптації та відновлення після інцидентів.

Міжнародні стандарти, зокрема ISO/IEC 27001 та рекомендації NIST, визначають базові підходи до забезпечення безпеки інформаційних систем, тоді як ISO 22301 акцентує увагу на безперервності діяльності. Європейські дослідження ENISA підкреслюють необхідність інтеграції кіберстійкості у системи управління критичною інфраструктурою.

Разом з тим, існуючі роботи українських науковців Коробейникова Ф., Бакалинського О., Гнатюка С., Сидоренка В., Селецького О., Костюченка Н. переважно зосереджені на IT-секторі або окремих аспектах кіберзахисту. Питання комплексної інформаційної стійкості підземних інженерних мереж, що поєднують фізичні та інформаційні компоненти, залишаються недостатньо дослідженими та потребують подальшого наукового опрацювання.

Мета статті – дослідження особливостей інформаційної стійкості об'єктів підземних інженерних мереж, визначення її основних складових та

ISSN 2786-6025 Online

обґрунтування комплексного підходу до забезпечення стійкого функціонування таких систем в умовах сучасних загроз.

Виклад основного матеріалу.

Стійкість (resilience) – це властивість системи зберігати або відновлювати свої ключові функції під впливом внутрішніх та зовнішніх негативних факторів. Стійкість є багатовимірним поняттям, застосовується як у природничих та соціальних науках, так і в інженерії, інформаційних та критично значущих системах [1-2].

У контексті інформаційних систем стійкість означає здатність:

– протистояти загрозам та відмовам;
– зберігати працездатність та цілісність даних;
– швидко відновлювати функціонування після інцидентів;
– адаптуватися до змін у навколишньому середовищі [3-4].

Стійкість виходить за межі традиційної концепції безпеки, оскільки включає не тільки захист від атак або відмов, але й спроможність системи до адаптації, самовідновлення та прогнозування потенційних ризиків [5].

Наукова та практична література виділяє кілька основних видів стійкості залежно від об’єкта та характеру впливу:

1. Фізична стійкість – здатність об’єкта протистояти фізичним навантаженням, пошкодженням або руйнуванню. Наприклад, трубопровід або теплотраса, що витримує гідравлічний удар або механічне пошкодження [6].

2. Інформаційна стійкість – здатність системи підтримувати цілісність, доступність та достовірність інформації при збоях або кібератаках. Наприклад, SCADA-системи підземних мереж, які продовжують працювати навіть при відмові частини датчиків [7].

3. Кіберстійкість – вид інформаційної стійкості, орієнтований на захист цифрових і мережевих систем від кібератак і забезпечення безперервності сервісів. Наприклад, резервні сервери та шифровані канали в IoT-системах моніторингу [8].

4. Організаційна стійкість – здатність організації зберігати управлінські та операційні функції під час криз або аварій. Наприклад, план реагування на аварії, навчання персоналу, розробка процедур резервного управління [3].

5. Екологічна та соціальна стійкість – здатність систем природного та соціального середовища відновлюватися після кризових подій. Наприклад, міські водопровідні системи, які швидко відновлюють подачу води після аварій чи стихійних лих [2].

Незалежно від виду, стійкість системи визначається наступними характеристиками:

– запобігання (preventive) – здатність знижувати ймовірність виникнення негативних подій;

ISSN 2786-6025 Online

– виявлення (detection) – своєчасне виявлення відхилень від норми;

– вдаптація (adaptive) – здатність змінювати поведінку у відповідь на загрози;

– Відновлення (recovery) – швидке відновлення функціонування після інцидентів [4, 5].

Таким чином, стійкість розглядається як комплексна властивість системи, що включає запобігання, реагування, адаптацію та відновлення, що робить її ключовим фактором безпеки та надійності в будь-якій критично значущій сфері [1, 3, 6].

Інформаційна стійкість визначається як здатність інформаційних систем підтримувати працездатність, цілісність і доступність навіть за умов реалізації внутрішніх або зовнішніх загроз. Дослідники підкреслюють, що це поняття виходить за межі традиційного захисту інформації та охоплює також адаптацію системи до кризових впливів і її відновлення після інцидентів [1].

Забезпечення інформаційної стійкості є комплексним процесом, що включає технічні, організаційні та управлінські заходи. Основною метою є створення таких умов, за яких інформаційна система зможе функціонувати безперервно навіть у разі кіберінцидентів або кризових ситуацій [9].

Одним із ключових напрямів є застосування технічних засобів захисту: шифрування, систем контролю доступу, резервного копіювання, мережевих екранів та IDS/IPS.

Такі підходи визначаються міжнародними стандартами ISO/IEC 27001 та рекомендаціями NIST [9-11].

Не менш важливим є впровадження систем моніторингу та реагування на інциденти, що забезпечують своєчасне виявлення атак та мінімізацію їх наслідків [12].

Організаційні заходи включають розробку політик безпеки, навчання персоналу, проведення аудитів та управління ризиками. Ці аспекти є критично важливими для забезпечення стійкості інформаційної інфраструктури.

У сучасній науковій літературі концепція resilience (стійкості) активно розвивається як окремий напрям у сфері кібербезпеки. Зокрема, дослідники зазначають, що стійкість інформаційних систем включає здатність до адаптації та самовідновлення, що є ширшим підходом порівняно з класичною моделлю захисту [3].

Європейські дослідження ENISA наголошують, що кіберстійкість має бути інтегрована у стратегію цифрового розвитку та управління критичною інфраструктурою [13].

Таким чином, інформаційна стійкість виступає не лише як елемент безпеки, але і як стратегічний ресурс, що забезпечує довіру до цифрових систем і стійкість організацій у кризових умовах [14].

ISSN 2786-6025 Online

Отже, інформаційна стійкість є комплексною характеристикою інформаційних систем, що охоплює запобігання загрозам, адаптацію до ризиків, реагування на інциденти та відновлення функціонування. Забезпечення інформаційної стійкості потребує інтеграції технічних, організаційних і нормативних підходів відповідно до міжнародних стандартів та сучасних наукових концепцій [10, 11, 13].

Критично значуща інфраструктура (КЗІ) охоплює системи, порушення функціонування яких може спричинити суттєві негативні наслідки для держави, економіки та безпеки населення. До таких об'єктів належать енергетичні системи, транспортні мережі, фінансовий сектор, телекомунікації, системи охорони здоров'я та державного управління. Інформаційні технології стали основою функціонування цих сфер, що підвищує їх залежність від кіберпростору та актуалізує проблему забезпечення інформаційної стійкості [4], [13, 15].

У сучасних умовах критична інфраструктура є однією з основних цілей кібератак, оскільки її виведення з ладу може призвести до масштабних соціально-економічних криз. Саме тому забезпечення інформаційної стійкості КЗІ є стратегічним пріоритетом державної політики та міжнародної безпеки [5].

Інформаційна стійкість критично значущої інфраструктури визначається як здатність її інформаційних систем підтримувати безперервність ключових функцій, зберігати працездатність та забезпечувати швидке відновлення після кіберінцидентів або деструктивних впливів [1].

На відміну від традиційного підходу до інформаційної безпеки, який зосереджується переважно на захисті від загроз, концепція resilience передбачає комплексну модель, що включає: запобігання атакам; адаптацію до змін у середовищі; реагування на інциденти; відновлення функціонування після порушень.

Таким чином, інформаційна стійкість КЗІ є не лише технічною характеристикою, але й системною властивістю, що визначає здатність держави та суспільства витримувати кризові впливи.

Інформаційні системи критично значущих об'єктів піддаються широкому спектру загроз, серед яких найбільш поширеними є:

– атаки на промислові системи управління (ICS/SCADA);
– цілеспрямовані кібератаки типу APT;
– порушення ланцюгів постачання програмного забезпечення;
– деструктивні атаки із застосуванням шкідливого ПЗ;
– інформаційно-психологічний вплив та гібридні загрози [13, 5].

Європейські дослідження ENISA наголошують, що критична інфраструктура повинна розглядатися як пріоритетний сектор для впровадження кіберстійких архітектур та систем моніторингу [13].

ISSN 2786-6025 Online

Забезпечення інформаційної стійкості критично значущої інфраструктури є багаторівневим процесом, що включає технічні, організаційні та нормативні механізми.

Технічна складова передбачає застосування сучасних засобів кіберзахисту: сегментації мережі, систем виявлення вторгнень, резервного копіювання, криптографічного захисту та постійного моніторингу. Важливу роль відіграють міжнародні стандарти, зокрема ISO/IEC 27001, які регламентують вимоги до систем управління інформаційною безпекою. Організаційні заходи включають управління ризиками, навчання персоналу, аудит безпеки та розробку планів реагування на інциденти. Стандарти ISO 22301 визначають необхідність забезпечення безперервності діяльності як ключового елементу стійкості.

Підземні інженерні мережі є критично важливими об'єктами інфраструктури, що забезпечують життєдіяльність міст і промислових підприємств. До них належать:

– водопровідні та каналізаційні системи;
– газопроводи та нафтопроводи;
– теплотраси;
– системи електропостачання та телекомунікаційних кабелів, прокладених під землею.

Ці системи характеризуються:

– фізичною розподіленістю на великі відстані;
– обмеженим доступом (часто важкодоступні або закриті для оперативного втручання);
– залежністю від безперервності функціонування (збої швидко призводять до соціально-економічних наслідків);
– поєднанням фізичних і інформаційних систем управління (SCADA, датчики тиску/температури, системи моніторингу витоків).

Тому забезпечення інформаційної стійкості для таких мереж має комплексний характер.

Для підземних інженерних мереж інформаційна стійкість може розглядатися як здатність системи управління та моніторингу забезпечувати безперервну, достовірну і своєчасну інформацію про стан мережі, навіть за умов загроз або відмов обладнання [1, 16].

Іншими словами, мова йде про:

1. Безперервність контролю та моніторингу – датчики тиску, витоків, температури, витрати енергії повинні працювати навіть під час аварій або часткових відмов мережі.

2. Захист даних і комунікацій – інформаційні канали SCADA та IoT-пристроїв не повинні бути піддані втручанню, фальсифікації або втраті даних.

ISSN 2786-6025 Online

3. Адаптація до аварійних умов – у разі відмови датчиків чи контролерів система повинна автоматично перенаправляти дані, активувати резервні канали або перевіряти цілісність показників.

4. Швидке відновлення працездатності – після аварій або кібератак чи фізичних атак система повинна швидко відновлювати функції моніторингу та управління.

Таким чином, інформаційна стійкість у підземних мережах не обмежується IT-захистом, а охоплює поєднання кіберзахисту, фізичного захисту та процедур реагування на аварії. Тут ключовими компонентами забезпечення є:

1. Технічні заходи:
– резервування датчиків та каналів передачі даних;
– шифрування та аутентифікація інформаційних потоків;
– впровадження SCADA-систем із кіберстійкими архітектурами.
2. Організаційні заходи:
– регламентація доступу до об’єктів і даних;
– навчання персоналу, включаючи аварійні процедури;
– регулярні аудити і тестування стійкості систем.
3. Моніторинг та прогнозування:
– виявлення аномалій у режимі реального часу;
– прогнозування потенційних відмов;
– інтеграція з системами раннього попередження аварій [3, 13].

Співставлення основних параметрів для забезпечення інформаційної стійкості КЗІ для IT-сектору та підземних інженерних мереж наведено в табл. 1.

Для підземних інженерних мереж інформаційна стійкість – це системна властивість, яка забезпечує:

безперервність та достовірність моніторингових даних;

своєчасне реагування на аварії чи атаки;

адаптацію та відновлення функцій управління мережами.

Забезпечення інформаційної стійкості таких мереж потребує поєднання кіберзахисту, фізичного захисту та організаційних процедур, що робить цей підхід міждисциплінарним і критично важливим для міської та національної безпеки.

Таблиця 1

Порівняння КЗІ підземних інженерних мереж з IT-сектором

Параметр	КЗІ IT	Підземні інженерні мережі
Основна функція стійкості	Захист даних і безперервність IT-послуг	Безперервність моніторингу та фізичного функціонування мереж

ISSN 2786-6025 Online

Параметр	КЗІ ІТ	Підземні інженерні мережі
Основні загрози	Кібератаки, відмови серверів	Аварії трубопроводів, витоки, відмови сенсорів, кібератаки на SCADA
Відновлення	Реплікація, резервні сервери, аварійне відновлення	Перенаправлення потоків, резервні контролери, аварійне обслуговування
Механізм адаптації	Автоматичне перемикання каналів, резервні мережі	Перенаправлення, перевірка датчиків, резервні системи управління

Серед систем моніторингу підземних мереж виділяють наступні:

1. SCADA-системи (Supervisory Control and Data Acquisition), які дозволяють збирати дані з датчиків тиску, витоку, рівня рідини, температури, управляти насосами та клапанами, а також формувати аварійні сповіщення. Приклади: Siemens SIMATIC SCADA, Schneider Electric EcoStruxure [1, 16, 17].

2. Системи детекції витоків:

HWM Water Management Systems – контроль тиску та витоків у водопроводах [6];

GasSecure – бездротові датчики газу для раннього виявлення витоків [19];

SmartBall (Xylem) – «плаваючі» пристрої для виявлення витоків і дефектів труб [7].

3. IoT-платформи: Sensus FlexNet, Kamstrup FlowIQ – бездротові мережі для збору даних з лічильників та датчиків, передача на сервери для аналітики [19, 20].

4. Аналітичні та ГІС-платформи:

Bentley OpenUtilities – прогнозування витоків, оптимізація насосів [21].

Esri ArcGIS Utility Network – інтеграція геоданих і SCADA для управління підземними мережами [22].

5. Практичні комерційні рішення:

SebaKMT® – раннє виявлення витоків із використанням акустичних і гідравлічних сенсорів [8].

Electro Scan Inc. – сканування трубопроводів для діагностики стану та передачі даних на сервер [23].

Для забезпечення інформаційної стійкості підземних мереж необхідне поєднання технічних, організаційних і аналітичних заходів:

1. Технічні: резервування датчиків, шифрування каналів, інтеграція SCADA та IoT.

2. Організаційні: регламентація доступу, навчання персоналу, аварійні процедури.

ISSN 2786-6025 Online

3. Аналітичні та прогнозні: виявлення аномалій, прогнозування аварій, інтеграція з ГІС.

Застосування таких комплексних підходів дозволяє забезпечити безперервність моніторингу та управління, швидке реагування на аварії та підтримку працездатності мереж у критичних умовах [12, 5].

Інформаційна стійкість підземних інженерних мереж забезпечує надійний збір і передачу даних, своєчасне виявлення аварій, адаптацію та відновлення функцій управління. Використання SCADA, IoT, аналітичних платформ та практичних технологій моніторингу робить системи підземних мереж стійкими до фізичних і кіберзагроз, що є критично важливим для безпеки міст і держави.

Висновки. Інформаційна стійкість підземних інженерних мереж є ключовою характеристикою їх надійності та безпеки, що визначає здатність систем забезпечувати безперервність моніторингу, достовірність даних і ефективне управління в умовах загроз.

Встановлено, що забезпечення інформаційної стійкості потребує інтеграції технічних, організаційних та аналітичних заходів, включаючи використання SCADA та IoT-систем, впровадження політик безпеки, навчання персоналу та застосування методів прогнозування аварій.

Особливості підземних мереж, зокрема їх розподіленість і обмежений доступ, зумовлюють необхідність створення кіберстійких архітектур і резервних механізмів управління.

Таким чином, підвищення інформаційної стійкості підземних інженерних мереж є стратегічним завданням, що потребує комплексного міждисциплінарного підходу та подальших наукових досліджень.

Література:

1. Korobeynikov F. O. Conceptual Framework for Information Systems Resilience // Problems in Programming. – 2023. – № 1. – С. 45–56. – URL: https://pp.isofts.kiev.ua/ojs1/article/view/611

2. Bakalynsky O., Gnatiuk S., Sydorenko V. Resilience of Information Infrastructure under Cyber Threats // Public Security and Public Safety Journal. – 2022. – № 4. – С. 22–31. – URL: https://psssj.eu/index.php/ojsdata/article/view/91

3. Korobeynikov F.O. Resilience paradigm development in the security domain. Èlektron. model. 2023, 45(4):88-110. https://doi.org/10.15407/emodel.45.04.088

4. Laprie J.-C. From Dependability to Resilience // IEEE/IFIP Conference on Dependable Systems and Networks. – 2008. – P. 1–12.

5. World Economic Forum. Global Cybersecurity Outlook. – Geneva, 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

6. Ramírez R. R. Sañudo-Fontaneda L. A. Human Aspects of Water Management at Impoverished Settlements. The Case of Doornkop, Soweto. *Water*, 2018, 10(3), 330; https://doi.org/10.3390/w10030330

ISSN 2786-6025 Online

7. Pure Technologies SmartBall® Inline Free-Swimming Inspection Platform. – URL: https://www.xylem.com/en-us/products--services/pipeline-assessment/smartball-inline-free-swimming-inspection-platform/

8. SebaKMT® – Leak Detection Systems. – URL: https://sebakmt.com/uk/produkte/monitoring-netzwerk/

9. ISO 22301:2019 Security and Resilience – Business Continuity Management Systems. – Geneva : ISO, 2019.

10. ISO/IEC 27001:2022 Information Security Management Systems – Requirements. – Geneva : ISO, 2022.

11. NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems. – Gaithersburg : NIST, 2020.

12. NIST SP 800-160 Systems Security Engineering. – Gaithersburg : NIST, 2018.

13. ENISA. Handbook for cyber stress tests. – European Union Agency for Cybersecurity, 2025. DOI: 10.2824/8248517

14. Boin A., Comfort L., Demchak C. The Rise of Resilience // International Journal of Critical Infrastructure Protection. – 2010. – Vol. 3(1). – P. 3–5.

15. Селецький, О. В., Костюченко Н.Д. Поняття та зміст інформаційної безпеки як складової національної безпеки / О. В. Селецький, Н. Д. Костюченко // Науковий вісник Сіверщини. Серія : Право. – 2025. - № 2 (25). - С. 98-106.

16. Gnatiuk, S., Bakalynsky, A., Myalkovsky, D., & Pakholchenko, D. (2022). Resilience and constantly of information infrastructure functioning within the national resilience system. Political Science and Security Studies Journal, 3(1), 26-31. https://doi.org/10.5281/zenodo.6385602

17. Siemens SIMATIC SCADA. – URL: https://www.siemens.com/en-us/products/scada/

18. GasSecure – A Dräger Company. – URL: https://www.gassecure.com/about/gassecure

19. SmartPoint 510M. – URL: https://cdn2.webdamdb.com/v6_md_RMhX7QoLlO2E.jpg.pdf?v=6

20. Kamstrup – flowIQ® 4200. – URL: https://www.kamstrup.com/en-en/product-centre/flowiq-4200

21. OpenUtilities Designer – Intelligent Design For Smarter Grids. – URL: https://www.bentley.com/software/openutilities-designer/

22. Esri ArcGIS Utility Network. – URL: https://www.esri.com/en-us/arcgis/products/arcgis-utility-network/overview

23. Electro Scan Inc. – Pipeline Assessment Technology. – URL: https://www.electroscan.com/

References:

1. Korobeynikov F. O. Conceptual Framework for Information Systems Resilience // Problems in Programming. – 2023. – № 1. – С. 45–56. – URL: https://pp.isofts.kiev.ua/ojs1/article/view/611

2. Bakalynsky O., Gnatiuk S., Sydorenko V. Resilience of Information Infrastructure under Cyber Threats // Public Security and Public Safety Journal. – 2022. – № 4. – С. 22–31. – URL: https://psssj.eu/index.php/ojsdata/article/view/91

3. Korobeynikov F.O. Resilience paradigm development in the security domain. Èlektron. model. 2023, 45(4):88-110. https://doi.org/10.15407/emodel.45.04.088

4. Laprie J.-C. From Dependability to Resilience // IEEE/IFIP Conference on Dependable Systems and Networks. – 2008. – P. 1–12.

ISSN 2786-6025 Online

5. World Economic Forum. Global Cybersecurity Outlook. – Geneva, 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

6. Ramírez R. R. Sañudo-Fontaneda L. A. Human Aspects of Water Management at Impoverished Settlements. The Case of Doornkop, Soweto. *Water*, 2018, 10(3), 330; https://doi.org/10.3390/w10030330

7. Pure Technologies SmartBall® Inline Free-Swimming Inspection Platform. – URL: https://www.xylem.com/en-us/products--services/pipeline-assessment/smartball-inline-free-swimming-inspection-platform/

8. SebaKMT® – Leak Detection Systems. – URL: https://sebakmt.com/uk/produkte/monitoring-netzwerk/

9. ISO 22301:2019 Security and Resilience – Business Continuity Management Systems. – Geneva : ISO, 2019.

10. ISO/IEC 27001:2022 Information Security Management Systems – Requirements. – Geneva : ISO, 2022.

11. NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems. – Gaithersburg : NIST, 2020.

12. NIST SP 800-160 Systems Security Engineering. – Gaithersburg : NIST, 2018.

13. ENISA. Handbook for cyber stress tests. – European Union Agency for Cybersecurity, 2025. DOI: 10.2824/8248517

14. Boin A., Comfort L., Demchak C. The Rise of Resilience // International Journal of Critical Infrastructure Protection. – 2010. – Vol. 3(1). – P. 3–5.

15. Seletskyi, O. V., Kostiuchenko N. D. Poniattia ta zmist informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky / O. V. Seletskyi, N. D. Kostiuchenko // Naukovyi visnyk Sivershchyny. Seriia: Pravo. – 2025. – № 2 (25). – S. 98–106. [in Ukrainian].

16. Gnatiuk, S., Bakalynsky, A., Myalkovsky, D., & Pakholchenko, D. (2022). Resilience and constantly of information infrastructure functioning within the national resilience system. Political Science and Security Studies Journal, 3(1), 26-31. https://doi.org/10.5281/zenodo.6385602

17. Siemens SIMATIC SCADA. – URL: https://www.siemens.com/en-us/products/scada/

18. GasSecure – A Dräger Company. – URL: https://www.gassecure.com/about/gassecure

19. SmartPoint 510M. – URL: https://cdn2.webdamdb.com/v6_md_RMhX7QoLlO2E.jpg.pdf?v=6

20. Kamstrup – flowIQ® 4200. – URL: https://www.kamstrup.com/en-en/product-centre/flowiq-4200

21. OpenUtilities Designer – Intelligent Design For Smarter Grids. – URL: https://www.bentley.com/software/openutilities-designer/

22. Esri ArcGIS Utility Network. – URL: https://www.esri.com/en-us/arcgis/products/arcgis-utility-network/overview

23. Electro Scan Inc. – Pipeline Assessment Technology. – URL: https://www.electroscan.com/

Дата першого надходження статті до видання: 09.04.2026
Дата прийняття статті до друку після рецензування: 22.04.2026

Журнал

«Наука і техніка сьогодні»

Випуск № 4(58) 2026

Формат 60х90/8. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 8,2. Наклад 100 прим.

Видавець:
Громадська наукова організація «Всеукраїнська асамблея докторів наук з державного управління»
Свідоцтво серія ДК №4957 від 18.08.2015 р., Андріївський узвіз, буд.11, оф 68, м. Київ, 04070.