МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Міністерство освіти і науки України
Український державний університет імені Михайла Драгоманова
Факультет технологій та дизайну
Кафедра професійної освіти
Інститут модернізації змісту освіти
Харківський національний університет імені В.Н . Каразіна
Кафедра гігієни та соціальної медицини
Харківський національний автомобільно-дорожній університет
Кафедра метрології та безпеки життєдіяльності

ПРОБЛЕМИ ЦИВІЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ ТА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ: СУЧАСНІ РЕАЛІЇ УКРАЇНИ

Матеріали
XII Всеукраїнської заочної
науково – практичної конференції
(30 квітня 2026 року, м. Київ)

КИЇВ 2026

УДК 355.58
ББК 68.69
П78
Редакційна колегія:

Шмалєй С.В. - доктор педагогічних наук., професор (головний редактор);
Яшанов С.М. - доктор педагогічних наук., професор (відповідальний редактор);
Шевченко В.В. – кандидат педагогічних наук, професор (заступник відповідального редактора)
Богатов О.І.- кандидат технічних наук, професор;
Володченкова Н.В. -кандидат технічних наук, доцент;
Виноградчий В.І. – доктор економічних наук, професор;
Гвоздій С.П.–доктор педагогічних наук, професор;
Дашковська О.В - кандидат хімічних наук, доцент;
Крутов В.В.- доктор юридичних наук, професор;
Мазепа М.А. – доктор медичних наук, професор;
Міхановська Н.Г.- доктор медичних наук, ст. науковий співробітник
Федорчук- Мороз В.І. - кандидат технічних наук, доцент;
Литвиновський Є.Ю. – кандидат педагогічних наук, ст. науковий співробітник
Редька І.В.- кандидат біологічних наук, доцент;
Слюсаренко Н.В. – доктор педагогічних наук, професор;
Постолатій Т.О. – начальник штабу цивільного захисту університету імені Михайла Драгоманова,(відповідальний секретар).

Затверджено до друку Організаційним комітетом XII Всеукраїнської заочної науково-практичної конференції «Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України»

Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України: Матеріали XII Всеукраїнської заочної науково - практичної конференції. Київ: УДУ імені Михайла Драгоманова, 2026 . – 205 с. Електронне видання

ISBN 978-966-931-352-2

Матеріали конференції висвітлюють результати різноспрямованих теоретичних і прикладних різноспрямованих досліджень в сфері цивільного захисту, розкривають сучасний стан, напрями та перспективи розвитку освіти в галузі цивільної безпеки та формування культури безпеки життєдіяльності

УДК 355.58
ББК 68.69
П78

ISBN 978-966-931-352-2

© Автори статей, 2026
© Український державний університет імені Михайла Драгоманова, 2026

районах, що характеризуються різноманітними інженерно-геологічними умовами. Стійкість цих споруд у великій мірі визначена сучасною геодинамікою – процесами і явищами, завдяки яким відбуваються деформації товщ гірських порід та зміни рельєфу Землі.

Провідним методом дослідження земної кори на основі дистанційних даних при геодинамічних дослідженнях є лінеаментний аналіз.

Лінеаменти – це лінійні аномалії рельєфу (і відповідні зображення на даних ДЗЗ), що генетично пов'язані з розломами і тріщинами земної кори, активними на неотектонічному етапі. Диз'юнктивні тектонічні структури, пов'язані з лінеаментами визначають рухомість блоків земної кори, фізико-механічні властивості ґрунтів, особливості циркуляції підземних вод, а також впливають на активність екзогенних геологічних процесів.

Дослідження проводилися на території розміщення магістрального газопроводу Лопушне-Росош. Він складається з двох ниток: Долина – Воловець і Долина – Россош.

Алювіально-делювіальні відклади, які залягають тут утворились завдяки змиву продуктів вивітрювання гірських порід вздовж схилів дощовими та талими водами. Ці відклади являють собою сірувато-жовту масу, яка складається із дрібних частинок ґрунту та крупноуламкового матеріалу. В долинах річок утворились дернові ґрунти.

Ландшафт території, зокрема, рельєф, формує особливості зображень на космічних знімках, які визначені поступовими та імпульсними, вертикальними та горизонтальними рухами земної кори на цій території. Аналізуючи особливості природно-територіальних комплексів, можна відтворити геодинамічну модель досліджуваного регіону.

Результатом дешифрування та формалізованої обробки космічних знімків із виділенням прямолінійних елементів зображення є вихідна схема лінеаментів. Розташування лінеаментів, особливо у платформених регіонах, не дозволяє однозначно виявити розташування тектонічних дислокацій, тому вихідна схема лінеаментів повинна підлягати подальшій обробці. Завданням перетворення вихідної схеми лінеаментів є перехід до континуального поля щільності лінеаментів, яке відображає просторові неоднорідності тектонічних напружень. При цьому головним завданням аналізу залишається виявлення розломів і геодинамічних зон.

За допомогою запропонованої методики з використанням ГІС побудовано карти загальної щільності лінеаментів; частоти лінеаментів; щільності лінеаментів певних напрямків.

На основі отриманих результатів створено інтегральну карту геодинамічних ризиків у межах ділянки магістрального газопроводу Лопушне-Росош з погляду надійності експлуатації газотранспортної системи.

Таким чином, ділянки, де траса трубопроводу перетинає геодинамічно активні зони, потребують особливої уваги, впровадження додаткових заходів з інженерного захисту трубопроводу та його інфраструктури.

ТРАНСФОРМАЦІЯ ПІДХОДІВ ДО МЕРЕЖЕВОГО ЗАХИСТУ ЯК ОСНОВА ЦИВІЛЬНОЇ КІБЕРБЕЗПЕКИ

к.п.н., доц. Ткаченко Л. А., Степанчук Є. Д.
Український державний університет імені Михайла Драгоманова
l.a.tkachenko@udu.edu.ua

Вступ. Кібербезпека – це захист у цифровому середовищі: даних, процесів застосунків і мереж. Якщо розглянути бізнес-середовищі тоді домінує думка, що кібербезпека – це виключно захист від атак. Практика міжнародна показує зовсім інше.

Захист – може бути тільки один із елементів. А сучасний підхід базується на трьох складових: запобігання, виявлення та реагування і відновлення.

Кіберпростір це середовище, яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, з використанням мережі Інтернет та інших глобальних мереж передачі даних.

Основна частина. Забезпечення кібербезпеки вимагає переосмислення класичної тріади інформаційної безпеки (Конфіденційність, Цілісність, Доступність) під кутом зору захисту цивільного населення. Згідно з аналітичними звітами (зокрема даними ENISA), однією з найпоширеніших загроз залишаються DDoS-атаки, які порушують саме *доступність* послуг. Відмова в обслуговуванні інформаційних ресурсів екстрених служб чи систем оповіщення несе пряму загрозу життю громадян.

Українська нормативно-правова база, зокрема Постанова КМУ № 518 та національний стандарт ДСТУ ISO/IEC 27001:2023, регламентує жорсткі вимоги до архітектурної сегментації мереж та вимагає впровадження ризикорієнтованого підходу [2, 3]. Проте практика показує, що традиційна периметральна модель захисту, яка ґрунтується на припущенні абсолютної довіри до внутрішньої мережі, більше не здатна ефективно протистояти сучасним витонченим векторам атак.

Найбільш дієвим технологічним рішенням для захисту інфраструктур, від яких залежить населення, є впровадження архітектури нульової довіри (Zero Trust Architecture – ZTA) [7]. Модель ZTA базується на принципі «Assume Breach» (передбачення того, що компрометація вже сталася) і вимагає безперервної, динамічної верифікації кожного запиту на доступ до ресурсів. Це критично важливо в умовах гібридних середовищ та масового використання населенням і підприємствами пристроїв Інтернету речей (IoT), які часто мають базові вразливості.

Окрім технологічного виміру (впровадження систем IDS/IPS, NAC, сучасних протоколів автентифікації типу TACACS+), критичним елементом кіберзахисту є освітньо-просвітницький напрям. Формування стійких навичок кібергігієни та цифрової компетентності у громадян дає змогу мінімізувати ризики, пов'язані з методами соціальної інженерії та фішингом, які активно використовується в інформаційно-психологічних операціях [7, С.29, 49].

Також необхідно знати про файли з розширенням .scr (screensaver/екранні заставки). Вони фактично є виконуваними файлами та не обмежуються лише законним використанням. Це дає змогу зловмисникам вбудовувати в них шкідливий код: кейлогери, програми-вимагачі або інструменти для віддаленого доступу. Завдяки системній довірі Windows до цього формату та використанню методів обфускації (заплутування коду), шкідливе навантаження легко проходить крізь початкові фільтри безпеки, ідентифікуючись як звичайна анімація. Контрольований експеримент із використанням інструменту Phantom Evasion довів, що запуск такого файлу миттєво надає хакеру повний віддалений доступ до системи через зворотну оболонку (reverse shell). Складність боротьби з цим вектором атаки полягає в тому, що легальний статус .scr-файлів ускладнює роботу антивірусів, які базуються на сигнатурному аналізі [6].

Ще приклад зламу через легітимний інструмент SQL-ін’єкція (SQLi), яка залишається однією з найбільш критичних загроз для вебдодатків, оскільки вона дає змогу зловмисникам маніпулювати запитами до бази даних через вразливі поля введення користувача. Шляхом впровадження шкідливого SQL-коду хакери отримують можливість обходити механізми автентифікації, переглядати конфіденційні записи, змінювати або навіть видаляти дані, що підриває цілісність усієї системи. Залежно від способу отримання даних, виділяють прямі ін’єкції (In-band), сліпі (Inferential), що базуються на логічних відповідях сервера, та позасмугові (Out-of-band). Основним методом протидії цій вразливості є використання параметризованих запитів (prepared statements), які чітко розмежовують код запиту та дані користувача, а також впровадження суворої валідації вхідних даних і принципу найменших привілеїв для доступу до бази даних [8].

Висновки. Гарантування інформаційної безпеки населення вимагає комплексної ешелонованої системи захисту. Відмова від застарілих периметральних моделей на користь адаптивних стратегій (Zero Trust), суворе дотримання національних стандартів кіберзахисту та підвищення загальної цифрової обізнаності громадян.

Список використаних джерел:

1. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро, 2020. URL: https://er.dduvs.edu.ua/handle/123456789/4206
2. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2022, IDT). [Чинний від 2023–08–22]. Київ : ДП «УкрНДНЦ», 2023. URL: https://factumcentr.com.ua/certificate-iso-27001/
3. Постанова КМУ від 19.06.2019 № 518 (із змінами) «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури». URL: https://zakononline.ua/documents/show/380155___696066
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (редакція станом на 19.10.2025) [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Смірнов О.А., Конопліцька-Слободенюк О.К. та ін. Інформаційна безпека в комп'ютерних мережах : навч. посіб. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/73209786-0b68-4fc2-8338-a86137bf992c/content
6. Abdallah Alhajeid. Weaponizing Screen Savers: A Deep Dive Into SCR File Exploitation 27.08.2024. WIZARDcyber [Електронний ресурс]. URL: https://wizardcyber.com/weaponizing-screen-savers-a-deep-dive-into-scr-file-exploitation/
7. Rose S., Borchert O., Mitchell S., Connelly S. NIST Special Publication 800-207 Zero Trust Architecture. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

What Is an SQL Injection? [Electronic resource] // Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/sql-injection

ОСОБЛИВОСТІ ВРАХУВАННЯ ВНУТРІШНІХ ЗАГРОЗ НА ПРОЯВ ІНШИХ ЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В.

Національний університет «Київський авіаційний інститут»

mega_ovtr@ukr.net

Внутрішні загрози – це шкідливі для організації загрози, які походять від людей всередині організації, таких як працівники, колишні працівники, підрядники або ділові партнери, які мають інформацію про методи безпеки всередині організації, доступ до матеріалів, технологічних процесів або комп'ютерних системи чи інформації. В умовах воєнного стану вплив внутрішніх загроз на безпеку і стійкість об'єктів критичної інфраструктури (ОКІ) набуває ще більшої значущості та їх прояв може посилювати негативні наслідки реалізації природних, воєнних, техногенних загроз і кібератак.