ЗАБЕЗПЕЧЕННЯ ВІЙСЬК (СИЛ)

Стаття та будь-який пов'язаний з нею опублікований матеріал поширюється за ліцензією Creative Commons Attribution License (CC BY 4.0).
The article and any related published material are licensed under the Creative Commons Attribution License (CC BY 4.0).

УДК 004.056:528.9:355.40
DOI: https://doi.org/10.17721/2519-481X/2026/91-05

Анатолій ЛУКІЯНЧУК, старший науковий співробітник
ORCID ID: 0000-0002-5757-6196
email: anatolii.lukiianchuk@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Олександр КОРЕНЕЦЬ, кандидат географічних наук
ORCID ID: 0000-0001-6352-9591
e-mail: oleksandr.korenets@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Софія СОКОЛОВА, науковий співробітник
ORCID ID: 0009-0006-9691-9370
e-mail: sofia77sokolova@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Микола ЦИБА, старший викладач
ORCID ID: 0000-0002-7768-7213
e-mail: Kolia.Tsyba@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ГЕОПРОСТОРОВИХ ДАНИХ У ВІЙСЬКОВИХ ГЕОІНФОРМАЦІЙНИХ СИСТЕМАХ: ЗАГРОЗИ, ОЦІНЮВАННЯ РИЗИКІВ ТА МЕХАНІЗМИ ЗАХИСТУ

Вступ. ***Геопросторові дані є важливим інформаційним ресурсом сучасних військових геоінформаційних систем. Їх компрометація, викривлення або недоступність можуть безпосередньо впливати на достовірність оперативної картини та безпеку підрозділів. Тому захист геопросторових даних потребує окремого розгляду з урахуванням їхньої чутливості, динамічності, інтеграції з іншими військовими інформаційними системами та значення для управлінських процесів.***

Методи. ***У дослідженні застосовано аналіз і узагальнення наукових джерел, системний та структурно-функціональний аналіз процесів збирання, передавання, зберігання, оброблення та використання геопросторових даних. Для класифікації сценаріїв компрометації використано модель STRIDE – підміна ідентичності, модифікація даних, заперечення авторства або виконаних дій, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв; для порівняльного модельно-аналітичного оцінювання – DREAD – потенційна шкода, відтворюваність, легкість реалізації, охоплення користувачів і виявлюваність); для врахування організаційних вразливостей – OCTAVE – оцінювання критично важливих для діяльності загроз, ресурсів і вразливостей. Бальні оцінки DREAD визначають відносну критичність сценаріїв за уніфікованою п'ятибальною шкалою та не є статистичною оцінкою частоти реальних інцидентів. Підсумкову пріоритетність ризиків визначено матричним зіставленням імовірності реалізації та рівня впливу, розрахованих із компонентів DREAD.***

Результати. ***Визначено основні об'єкти інформаційного захисту військової геоінформаційної системи та сформовано послідовний аналітичний контур "об'єкт інформаційного захисту – STRIDE - DREAD – OCTAVE – матриця ризиків – механізм захисту". За DREAD найбільшу суму отримав сценарій атаки типу розподіленої відмови в обслуговуванні на геоінформаційний сервіс – 22 із 25 балів ("дуже високий" рівень). Високий рівень встановлено для несанкціонованої зміни координат об'єкта – 18 балів, компрометації облікового запису оператора – 18 балів, несанкціонованого внутрішнього копіювання конфіденційного геопросторового шару – 18 балів та підміни геопросторових даних у каналі передавання – 16 балів. У підсумковій матриці DDoS-атаку, спотворення координатної або атрибутивної інформації та підміну геопросторових даних віднесено до критичних ризиків, а компрометацію облікового запису й несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару - до високих.***

Висновки. ***Науковий результат дослідження полягає в розвитку методичного підходу до оцінювання ризиків інформаційної безпеки геопросторових даних у військових геоінформаційних системах шляхом послідовного поєднання визначення основних об'єктів інформаційного захисту, STRIDE-класифікації сценаріїв компрометації, їх модельно-аналітичного оцінювання за DREAD, урахування організаційних вразливостей за OCTAVE та формування матриці пріоритетності ризиків. Практичне значення підходу полягає у відтворюваному ранжуванні сценаріїв і обґрунтуванні черговості механізмів захисту: контролю доступу, криптографічного захисту, контролю цілісності, моніторингу інцидентів, резервування, реплікації та організаційних заходів.***

Ключові слова: геопросторові дані, військова геоінформаційна система, інформаційна безпека, ризики, захист даних.

Вступ

Геопросторові дані є одним із ключових інформаційних ресурсів сучасних військових геоінформаційних систем (далі – ГІС). Вони забезпечують просторове відображення обстановки, підтримують управління військами, планування

© Лукіянчук Анатолій, Коренець Олександр, Соколова Софія, Циба Микола, 2026

ISSN 2519-481X

операцій, логістичне забезпечення та прийняття рішень на різних рівнях військового управління. Їх значення визначається не лише обсягом інформації, а й їх значенням для аналізу місцевості, координації дій підрозділів, визначення маршрутів, позицій і зон відповідальності. У структурі військових інформаційних систем геопросторові дані виконують базову функцію, оскільки формують інформаційну основу актуальної оперативної картини.

Геопросторові дані поєднують координатні характеристики об'єктів з атрибутивною інформацією, яка відображає їх функціональний, інфраструктурний або оперативний зміст. У військовому середовищі такі дані можуть містити відомості про розташування військових об'єктів, інженерну інфраструктуру, маршрути переміщення, логістичні напрямки та інші елементи, компрометація яких прямо впливає на якість управлінських рішень і безпеку підрозділів. Через це їх захист не можна зводити до загального кіберзахисту інформаційної системи. Він потребує окремого розгляду з урахуванням властивостей самих даних, умов їх використання та наслідків їх компрометації (Das, P. et al., 2024; Burton, 2025).

Забезпечення інформаційної безпеки геопросторових даних у військових ГІС ускладнюється декількома обставинами. Ці дані мають високу прикладну цінність і значну чутливість. Вони функціонують у межах інтегрованого інформаційного середовища, де взаємодіють із системами управління військами, розвідки, навігації та спостереження. Військове середовище є динамічним, потребує оперативного оновлення відомостей і характеризується підвищеним рівнем кіберзагроз. За таких умов захист геопросторових даних вимагає системного поєднання аналізу загроз, оцінювання ризиків і впровадження взаємопов'язаних механізмів захисту (Si, D. et al., 2025).

Мета дослідження полягає в аналізі особливостей забезпечення інформаційної безпеки геопросторових даних у військових ГІС через розгляд їх функціональної ролі, структури загроз, підходів до оцінювання ризиків та механізмів захисту. Для досягнення цієї мети потрібно: визначити роль геопросторових даних у військових ГІС, систематизувати основні загрози їх інформаційній безпеці, розглянути підходи до оцінювання ризиків і обґрунтувати механізми захисту, що відповідають специфіці військового застосування.

Наукова новизна дослідження полягає в розвитку методичного підходу до оцінювання ризиків інформаційної безпеки геопросторових даних у військових ГІС, у межах якого послідовно поєднано визначення основних об'єктів інформаційного захисту, STRIDE-класифікацію сценаріїв компрометації, їх модельно-аналітичне оцінювання за DREAD, урахування організаційних вразливостей за OCTAVE та формування матриці пріоритетності ризиків для вибору механізмів захисту. Практичне значення підходу полягає у можливості відтворюваного ранжування сценаріїв за єдиними критеріями та обґрунтування черговості захисних заходів без ототожнення модельних оцінок зі статистичною частотою реальних кіберінцидентів.

Методи

Методологічну основу дослідження становить поєднання загальнонаукових і спеціальних методів, використаних для аналізу інформаційної безпеки геопросторових даних у військових геоінформаційних системах. Теоретичну базу формують аналіз і узагальнення наукових джерел у сфері захисту інформації, кібербезпеки та застосування геоінформаційних систем. Це дає змогу розглядати проблему в контексті життєвого циклу геопросторових даних, типових класів загроз і ризик-орієнтованого вибору механізмів захисту.

Для дослідження особливостей функціонування геопросторових даних у військових ГІС використано системний і структурно-функціональний аналіз. Це дозволяє розглядати процеси збору, передавання, зберігання, оброблення та використання геопросторових даних як єдину взаємопов'язану систему. Такий підхід є важливим, оскільки уразливості виникають не лише в окремих технічних вузлах, а й на стиках між каналами взаємодії, рівнями доступу, джерелами надходження інформації та процедурами її використання.

На початковому етапі дослідження було визначено основні об'єкти інформаційного захисту військової геоінформаційної системи (таблиця 1).

Таблиця 1

Основні об'єкти інформаційного захисту військової геоінформаційної системи

№ з/п	Основний об'єкт інформаційного захисту	Функціональне значення	Можливий наслідок компрометації
1	Геопросторова база даних	Зберігання координатної та атрибутивної інформації про об'єкти	Втрата достовірності просторової картини, спотворення даних
2	Цифрові картографічні шари	Відображення місцевості, об'єктів, маршрутів та зон відповідальності	Помилки у візуалізації обстановки та плануванні дій
3	Канали передавання геопросторових даних	Передавання оновленої інформації між елементами системи	Перехоплення, підміна або затримка критичних даних
4	Геоінформаційні сервіси	Надання доступу до картографічних і аналітичних ресурсів	Недоступність сервісів, порушення оперативної роботи
5	Облікові записи користувачів	Доступ до перегляду, редагування та адміністрування даних	Несанкціоновані дії, зловживання доступом, витік інформації
6	Засоби контролю цілісності та протоколювання дій користувачів	Фіксація змін, аудит дій і виявлення порушень	Неможливість виявлення викривлень і несанкціонованих змін

Джерело: складено авторами.

У межах цієї роботи словосполучення "основні об'єкти інформаційного захисту" використовується як операційне позначення елементів системи, порушення конфіденційності, цілісності або доступності яких може безпосередньо впливати на достовірність оперативної картини, доступність геоінформаційних сервісів та якість управлінських рішень. Воно не розглядається як окрема нормативна категорія. До таких об'єктів віднесено

геопросторові бази даних, цифрові картографічні шари, канали передавання геопросторових даних, геоінформаційні сервіси, облікові записи користувачів та засоби контролю цілісності інформації. У подальшому STRIDE-аналізі цифрові картографічні шари розглядалися як інформаційна складова геопросторової бази даних, тоді як персонал в OCTAVE враховувався як організаційний фактор ризику, а не як окремий об'єкт інформаційного захисту. Такий поділ забезпечує узгодженість об'єктів аналізу між етапами дослідження.

Для оцінювання загроз і ризиків використано три взаємодоповнювальні підходи (Ouaissa, M. et al., 2025; Si, D. et al., 2025, Kausika, & van Altena, 2025): STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege – підміна ідентичності, модифікація даних, заперечення авторства або виконаних дій, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв), DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability – потенційна шкода, відтворюваність, легкість реалізації, охоплення користувачів і виявлюваність) та OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation – оцінювання критично важливих для діяльності загроз, ресурсів і вразливостей). STRIDE застосовано для початкової класифікації сценаріїв компрометації за характером впливу на систему; DREAD – для їх порівняльного модельно-аналітичного оцінювання; OCTAVE – для врахування організаційного контексту, режимів доступу, ролі персоналу та внутрішніх вразливостей. Така послідовність дає змогу перейти від ідентифікації об'єкта інформаційного захисту до пріоритизації ризику та обґрунтування відповідного механізму захисту.

Оцінювання за DREAD у цій роботі має модельно-аналітичний характер. Для кожного сценарію використано п'ять критеріїв із балами від 1 до 5: потенційна шкода (D), відтворюваність (R), легкість реалізації (E), охоплення користувачів (A) та виявлюваність (Di). Потенційна шкода характеризує масштаб можливих наслідків: 1 бал – локальні та відновлювані наслідки без втрати ключової функції; 3 – суттєве порушення окремого компонента або частини даних; 5 – наслідки, здатні спотворити оперативну картину або порушити безперервність управління. Відтворюваність відображає повторюваність сценарію: 1 – реалізація потребує виняткових умов; 3 – можлива за визначених і відтворюваних умов; 5 – легко повторюється за типової доступності цілі. Легкість реалізації характеризує необхідні ресурси та складність здійснення сценарію: 1 – потрібні складні спеціалізовані засоби, значні ресурси або привілейований доступ; 3 – потрібен помірний рівень технічних чи організаційних можливостей; 5 – сценарій реалізується з відносно низькою складністю або із застосуванням поширених засобів. Охоплення користувачів визначає масштаб впливу: 1 – окремий користувач або ізольований компонент; 3 – група користувачів чи підсистема; 5 – значна частина користувачів або система в цілому. Виявлюваність характеризує легкість виявлення потенційним суб'єктом атаки можливості реалізації сценарію: 1 – можливість складно виявити; 3 – вона виявляється за спеціалізованого аналізу; 5 – виявляється відносно легко за стандартних методів аналізу.

Інтегральний показник DREAD визначено як суму п'яти складових: S_DREAD = D + R + E + A + Di. Теоретичний діапазон становить від 5 до 25 балів. Для цієї роботи прийнято чотири інтервали відносної критичності: 5–9 балів – низький рівень; 10–14 – середній; 15–19 – високий; 20–25 – дуже високий. Таке групування використовується як внутрішня шкала порівняльного ранжування сценаріїв у межах запропонованої моделі. Наведені бальні значення не є статистичною оцінкою частоти реальних кіберінцидентів і не замінюють емпіричні дані експлуатації конкретної військової ГІС.

Для формування підсумкової матриці ризиків показник імовірності реалізації розраховано з компонентів DREAD як P = (R + E + Di) / 3, а рівень впливу – як I = (D + A) / 2. Значення від 1,00 до 2,00 віднесено до низького рівня, понад 2,00, але менше 4,00 – до середнього, від 4,00 до 5,00 – до високого. Підсумкову категорію визначено за матрицею "імовірність × вплив": поєднання низького рівня з низьким дає низький ризик; низького із середнім або середнього з низьким – середній; середнього із середнім, а також високого з низьким або низького з високим – високий; середнього з високим, високого із середнім або високого з високим – критичний. OCTAVE використано для інтерпретації організаційних умов і вибору захисних заходів; його результати не підміняють і не змінюють числові складові DREAD.

Результати

За результатами системного та структурно-функціонального аналізу встановлено, що для цілей інформаційного захисту геопросторові дані у військових ГІС доцільно розглядати через сукупність взаємопов'язаних компонентів, які виступають основними об'єктами інформаційного захисту та компрометація яких впливає на достовірність оперативної картини, доступність геоінформаційних сервісів і керованість інформаційного обміну. До таких об'єктів віднесено геопросторову базу даних, цифрові картографічні шари, канали передавання геопросторових даних, геоінформаційні сервіси, облікові записи користувачів та засоби контролю цілісності й протоколювання.

Аналіз сценаріїв компрометації показав, що загрози охоплюють порушення конфіденційності, цілісності та доступності, однак для військових ГІС особливе значення мають сценарії, здатні викривити координатну або атрибутивну інформацію чи зробити актуальні геопросторові дані недоступними. Саме такі наслідки безпосередньо змінюють якість просторового представлення обстановки та можуть порушувати безперервність інформаційного забезпечення управління.

Для подальшого порівняльного оцінювання відібрано п'ять сценаріїв, що репрезентують різні типи впливу на визначені об'єкти інформаційного захисту: несанкціоновану зміну координат об'єкта, підміну геопросторових даних у каналі передавання, атаку типу розподіленої відмови в обслуговуванні (англ. Distributed Denial of Service, DDoS) на геоінформаційний сервіс, компрометацію облікового запису оператора та несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару. Їх послідовне оцінювання за STRIDE, DREAD та OCTAVE становить основну частину власних результатів дослідження.

Модель STRIDE (таблиця 2) є придатною для початкової структуризації загроз за їх функціональним типом. Вона охоплює підміну, модифікацію даних, відмову від авторства, розкриття інформації, відмову в обслуговуванні та підвищення привілеїв. У контексті військових геоінформаційних систем ця модель дозволяє системно охопити основні сценарії компрометації геопросторових даних: від несанкціонованого отримання відомостей до спотворення просторової інформації чи блокування сервісів доступу. STRIDE виконує функцію аналітичної рамки, яка дозволяє виявити не лише факт наявності загрози, а й її місце у загальній архітектурі ризиків системи..

Таблиця 2

Віднесення основних типів загроз до об'єктів інформаційного захисту за підходом STRIDE

Об'єкт інформаційного захисту	S – Підміна	T – Модифікація	R – Заперечення авторства	I – Розкриття інформації	D – Відмова в обслуговуванні	E – Підвищення привілеїв
Геопросторова база даних	+	+	+	+	+	+
Канали передавання геопросторових даних	+	+	–	+	+	–
Геоінформаційний сервіс	–	–	–	+	+	–
Облікові записи користувачів	+	–	+	+	–	+
Засоби контролю цілісності	–	+	+	+	–	+

Джерело: складено авторами.

За результатами STRIDE-аналізу для порівняльного оцінювання за DREAD відібрано п'ять сценаріїв: несанкціоновану зміну координат об'єкта, підміну геопросторових даних у каналі передавання, DDoS-атаку на геоінформаційний сервіс, компрометацію облікового запису оператора та несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару. Бальні значення визначено за критеріями та інтервалами, описаними в розділі "Методи", а результати наведено в таблиці 3.

Таблиця 3

Порівняльне оцінювання основних сценаріїв загроз за підходом DREAD

Сценарій загрози	D – Потенційна шкода	R – Відтворюваність	E – Легкість реалізації	A – Охоплення користувачів	Di – Виявлюваність	Сума балів	Рівень ризику
Несанкціонована зміна координат об'єкта	5	3	3	4	3	18	Високий
Підміна геопросторових даних у каналі передавання	5	3	2	4	2	16	Високий
DDoS-атака на геоінформаційний сервіс	4	5	4	5	4	22	Дуже високий
Компрометація облікового запису оператора	4	4	3	3	4	18	Високий
Несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару	4	4	4	3	3	18	Високий

Джерело: складено авторами.

За сумою DREAD найвище значення отримала DDoS-атака на геоінформаційний сервіс – 22 із 25 балів, що відповідає дуже високому рівню. Несанкціонована зміна координат об'єкта, компрометація облікового запису оператора та несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару отримали по 18 балів, а підміна геопросторових даних у каналі передавання – 16 балів; усі чотири сценарії віднесено до високого рівня. Таким чином, DREAD-оцінювання показує одночасну значущість ризиків доступності, цілісності, контролю доступу та внутрішніх порушень.

Методологія OCTAVE доповнює цей аналіз урахуванням організаційного контексту функціонування системи. Її цінність полягає в тому, що вона зосереджується на об'єктах інформаційного захисту, сценаріях ризику та організаційних вразливостях, у тому числі пов'язаних із людським фактором. Для військових

систем це має особливе значення, оскільки ефективність захисту визначається не лише технічними параметрами, а й режимом доступу, регламентами, підготовкою персоналу та організацією контролю. Це дає можливість вийти за межі суто технічного аналізу й оцінити ризик у реальних умовах функціонування системи.

Застосування методології OCTAVE дало змогу доповнити технічний аналіз ризиків (таблиця 4) урахуванням організаційних умов функціонування військової геоінформаційної системи. Основну увагу було зосереджено на об'єктах інформаційного захисту, режимах доступу, ролі персоналу, внутрішніх вразливостях і можливих наслідках порушення регламентів роботи з геопросторовими даними.

Таблиця 4

Оцінювання організаційного контексту ризиків за підходом OCTAVE

Об'єкт інформаційного захисту	Організаційна вразливість	Потенційний сценарій ризику	Можливий наслідок
Геопросторова база даних	Недостатньо чітке розмежування прав доступу	Несанкціоноване редагування або видалення даних	Порушення цілісності інформації
Канали передавання геопросторових даних	Недостатній контроль захищеності каналів зв'язку	Підміна або перехоплення даних	Формування недостовірної просторової картини
Облікові записи користувачів	Недостатня стійкість процедур автентифікації	Компрометація акаунта	Несанкціонований доступ до системи
Геоінформаційний сервіс	Відсутність чіткого регламенту реагування на інциденти	Затримка локалізації атаки	Тривала недоступність сервісу
Персонал	Недостатній рівень підготовки з безпечної роботи з даними	Помилки користувачів або успішний фішинг	Витік або викривлення інформації

Джерело: складено авторами.

OCTAVE дозволив установити, що значна частина ризиків для геопросторових даних формується не лише через технічні уразливості, а й через особливості організації доступу, контролю, навчання персоналу та управління інцидентами. Це підтверджує необхідність поєднання технічних і організаційних механізмів захисту у військових ГІС.

Підсумкову матрицю пріоритетності сформовано за правилами, визначеними в розділі "Методи". Для DDoS-атаки P = (5 + 4 + 4) / 3 = 4,33, що відповідає високій імовірності, а I = (4 + 5) / 2 = 4,50 – високому впливу; підсумкова категорія є критичною. Для спотворення координатної інформації P = (3 + 3 + 3) / 3 = 3,00 – середня імовірність, I = (5 + 4) / 2 = 4,50 – високий вплив; підсумкова категорія також є критичною. Для несанкціонованого внутрішнього копіювання конфіденційного геопросторового шару P = (4 + 4 + 3) / 3 = 3,67 та I = (4 + 3) / 2 = 3,50, тобто обидва показники відповідають середньому рівню, а підсумкова категорія – високому ризику. Наведені приклади демонструють відтворюваний перехід від компонентів DREAD до таблиці 5.

Таблиця 5

Матриця пріоритетності ризиків для військової геоінформаційної системи

Сценарій ризику	Ймовірність реалізації	Рівень впливу	Підсумкова категорія ризику
DDoS-атака на геоінформаційний сервіс	Висока	Високий	Критичний
Спотворення координатної або атрибутивної інформації	Середня	Високий	Критичний
Підміна геопросторових даних у каналі передавання	Середня	Високий	Критичний
Компрометація облікового запису користувача	Середня	Середній	Високий
Несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару	Середня	Середній	Високий

Джерело: складено авторами.

Підсумкова матриця відносить DDoS-атаку на геоінформаційний сервіс, спотворення координатної або атрибутивної інформації та підміну геопросторових даних у каналі передавання до критичних ризиків. Компрометацію облікового запису користувача та несанкціоноване внутрішнє копіювання конфіденційного геопросторового шару віднесено до високих ризиків. Саме ця пріоритетність використана далі для обґрунтування механізмів захисту.

Дискусія і висновки

Зіставлення модельно-аналітичного оцінювання за DREAD із підсумковою матрицею ризиків показує, що сумарний бал і кінцева категорія ризику виконують різні аналітичні функції. DREAD характеризує відносну критичність сценарію за сукупністю п'яти критеріїв, тоді як матриця окремо враховує співвідношення імовірності реалізації та рівня впливу. Тому сценарії з різними сумарними балами можуть належати до однакової підсумкової категорії ризику. Це обґрунтовує використання двоетапного оцінювання та дає змогу уникнути висновків, заснованих лише на одному інтегральному показнику.

Отримані результати узгоджуються із загальною логікою системного аналізу кіберризиків, захисту цілісності просторової інформації та врахування специфіки застосування геоінформаційних систем, представленою в попередніх дослідженнях (Si, D. et al., 2025; Kausika, & van Altena, 2025; Філіппов, Балагур, & Башнянин, 2025; Chipatiso, 2025). Методичний внесок цієї роботи полягає в адаптації такої логіки до військових ГІС через послідовне пов'язування основного об'єкта інформаційного захисту, типу загрози, модельної оцінки

ризику, організаційної вразливості та відповідного механізму захисту. Запропонований контур "об'єкт інформаційного захисту – STRIDE – DREAD – OCTAVE – матриця ризиків – механізм захисту" робить перехід від ідентифікації загрози до визначення захисного пріоритету прозорим і відтворюваним у межах заданих критеріїв.

Практичне значення отриманих результатів полягає у можливості співвідносити домінуючий характер ризику з відповідними класами заходів захисту. Для несанкціонованого доступу такими заходами є криптографічний захист, розмежування повноважень і багатофакторна автентифікація; для спотворення геопросторових даних – контроль цілісності, цифрові підписи, контрольні суми та журналювання змін; для порушення доступності – резервне копіювання, реплікація та процедури відновлення. Моніторинг і реагування на інциденти можуть підтримуватися системами управління інформацією та подіями інформаційної безпеки, а організаційні вразливості потребують регламентації доступу, аудиту й підготовки персоналу. У межах цієї статті зазначені заходи обґрунтовано аналітично; їх ефективність для конкретної реалізації військової ГІС експериментально не оцінювалася.

Таким чином, проведене дослідження підтверджує доцільність ризик-орієнтованого захисту геопросторових даних у військових ГІС із одночасним урахуванням технічних та організаційних чинників. Запропонована послідовність оцінювання забезпечує формалізований перехід від визначення об'єктів інформаційного захисту та сценаріїв їх компрометації до встановлення пріоритетів захисних заходів. Найбільше практичне значення мають механізми, спрямовані на збереження цілісності й доступності геопросторових даних, доповнені контролем доступу та організаційними процедурами.

Обмеженням дослідження є модельно-аналітичний характер кількісного оцінювання: бали DREAD відображають відносну критичність сценаріїв у межах заданої шкали й не є статистикою фактичних інцидентів у конкретній військовій ГІС. Подальші дослідження доцільно спрямувати на верифікацію критеріїв із використанням експертного оцінювання та, за наявності доступних і допустимих до використання даних, емпіричної інформації про інциденти безпеки.

Внесок авторів: Анатолій Лукіянчук – концептуалізація, написання – перегляд і редагування; Олександр Коренець – методологія, аналіз джерел, написання – оригінальна чернетка; Софія Соколова – збирання вихідних даних, написання – перегляд і редагування; Микола Циба – написання – перегляд і редагування.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Das, P., Asif, M. R. A., Jahan, S., Ahmed, K., Bui, F. M., & Khondoker, R. (2024). STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. *Vehicles, 6(3)*. https://doi.org/10.3390/vehicles6030054

Ouaissa, M., Ouaissa, M., Nadifi, Z., El Himer, S., Al Masmoudi, Y., & Kartit, A. (2025). A framework for cyber threat modeling and risk assessment in smart city environments. *Frontiers in Computer Science, 7*. https://doi.org/10.3389/fcomp.2025.1647179

Burton, S. L. (2025). Business intelligence and GPS spoofing: Navigating cybersecurity challenges in digital surveillance systems. HOLISTICA *Journal of Business and Public Administration. 16(1).* https://doi.org/10.2478/hjbpa-2025-0008

Si, D., Jiang, B., Xia, Q., Li, T., Wang, X., & Liu, J. (2025). Cyber Potential Metaphorical Map Method Based on GMap. *International Journal of Geo-Information, 14(2)*. https://doi.org/10.3390/ijgi14020046

Kausika, B. B., & van Altena, V. (2025). GeoAI in Topographic Mapping: Navigating the Future of Opportunities and Risks. *International Journal of Geo-Information, 14(8).* https://doi.org/10.3390/ijgi14080313

Філіппов, М., Балагур, Л., & Башнянин, О. (2025). Інтеграція цифрових топографічних даних у бойове планування підрозділів тактичної ланки: виклики та перспективи. *Національні інтереси України, 5(10).* https://dspace.nadpsu.edu.ua/bitstream/123456789/6588/1/Natsionalni%20interesy_5_10_2025.pdf

Chipatiso, E. (2025). Application of GIS and artificial intelligence in military operations: Prospects and challenges. *Southern African Journal of Security, 3.* https://unisapressjournals.co.za/index.php/sajs/article/view/15984

References

Das, P., Asif, M. R. A., Jahan, S., Ahmed, K., Bui, F. M., & Khondoker, R. (2024). STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. *Vehicles, 6(3)*. https://doi.org/10.3390/vehicles6030054

Ouaissa, M., Ouaissa, M., Nadifi, Z., El Himer, S., Al Masmoudi, Y., & Kartit, A. (2025). A framework for cyber threat modeling and risk assessment in smart city environments. *Frontiers in Computer Science, 7*. https://doi.org/10.3389/fcomp.2025.1647179

Burton, S. L. (2025). Business intelligence and GPS spoofing: Navigating cybersecurity challenges in digital surveillance systems. HOLISTICA *Journal of Business and Public Administration. 16(1).* https://doi.org/10.2478/hjbpa-2025-0008

Si, D., Jiang, B., Xia, Q., Li, T., Wang, X., & Liu, J. (2025). Cyber Potential Metaphorical Map Method Based on GMap. *International Journal of Geo-Information, 14(2)*. https://doi.org/10.3390/ijgi14020046

Kausika, B. B., & van Altena, V. (2025). GeoAI in Topographic Mapping: Navigating the Future of Opportunities and Risks. *International Journal of Geo-Information, 14(8).* https://doi.org/10.3390/ijgi14080313

Filippov, M., Balahur, L., & Bashnianyn, O. (2025). Integration of digital topographic data into tactical-level combat planning: Challenges and prospects. *National Interests of Ukraine, 5(10).* [in Ukrainian]. https://dspace.nadpsu.edu.ua/bitstream/123456789/6588/1/Natsionalni%20interesy_5_10_2025.pdf

Chipatiso, E. (2025). Application of GIS and artificial intelligence in military operations: Prospects and challenges. *Southern African Journal of Security, 3.* https://unisapressjournals.co.za/index.php/sajs/article/view/15984

Отримано редакцією журналу / Received: 24.04.26
Прорецензовано / Revised: 15.05.26
Схвалено до друку / Accepted: 18.06.26
Опубліковано / Published: 30.06.26

Anatolii LUKIIANCHUK, Senior Researcher
ORCID ID: 0000-0002-5757-6196
email: anatolii.lukiianchuk@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Oleksandr KORENETS, PhD (Geogr.)
ORCID ID: 0000-0001-6352-9591
e-mail: oleksandr.korenets@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Sofiia SOKOLOVA, Researcher
ORCID ID: 0009-0006-9691-9370
e-mail: sofia77sokolova@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola Tsyba, Senior Lecturer
ORCID ID: 0000-0002-7768-7213
e-mail: Kolia.Tsyba@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ENSURING THE INFORMATION SECURITY OF GEOSPATIAL DATA IN MILITARY GEOGRAPHIC INFORMATION SYSTEMS: THREATS, RISK ASSESSMENT, AND PROTECTION MECHANISMS

Background. *Geospatial data constitutes a critical information resource within modern military geographic information systems (GIS). Its compromise, distortion, or unavailability can directly impact the reliability of the operational picture and the security of military units. Consequently, the protection of geospatial data necessitates dedicated consideration, accounting for its sensitivity, dynamism, integration with other military information systems, and significance in command-and-control processes.*

Methods. *The study employs the analysis and synthesis of scientific literature, alongside a systemic and structural-functional analysis of the processes involved in the collection, transmission, storage, processing, and utilization of geospatial data. To classify compromise scenarios, the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) was utilized; for comparative model-analytical assessment, the DREAD model (Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability) was applied; and to account for organizational vulnerabilities, the OCTAVE framework (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was incorporated. The DREAD scoring system determines the relative criticality of scenarios using a standardized five-point scale and does not represent a statistical estimate of actual incident frequency. The final risk prioritization was established through a matrix correlation of the likelihood of occurrence and the level of impact, derived from the DREAD components.*

Results. *The primary targets of information protection within a military GIS were identified, and a sequential analytical framework was developed: "information protection target – STRIDE – DREAD – OCTAVE – risk matrix – defense mechanism." Based on the DREAD evaluation, the scenario involving a Distributed Denial of Service (DDoS) attack on a geoinformation service attained the highest score – 22 out of 25 points (a "very high" risk level). A "high" risk level was assigned to the unauthorized alteration of object coordinates (18 points), operator account compromise (18 points), unauthorized internal duplication of a confidential geospatial layer (18 points), and the tampering of geospatial data within the transmission channel (16 points). In the final risk matrix, DDoS attacks, distortion of coordinate or attribute information, and geospatial data tampering were categorized as critical risks, whereas account compromise and the unauthorized internal duplication of confidential geospatial layers were categorized as high risks.*

Conclusions. *The scientific contribution of this study lies in the advancement of a methodological approach for assessing information security risks to geospatial data in military GIS. This is achieved through the sequential integration of identifying primary information protection targets, classifying compromise scenarios via STRIDE, conducting a model-analytical assessment using DREAD, factoring in organizational vulnerabilities via OCTAVE, and formulating a risk prioritization matrix. The practical significance of this approach consists in the reproducible ranking of threat scenarios and the substantiation of the implementation sequence for defense mechanisms: access control, cryptographic protection, integrity control, incident monitoring, data backup, replication, and organizational measures.*

Keywords: *geospatial data, military Geographic Information System (GIS), information security, risk assessment, data protection.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.