Захист даних в автоматизованих системах управління земельними ресурсами органів місцевого самоврядування

https://doi.org/10.31713/MCIT.2025.038

Василь Дрозд
Національний університет водного господарства та природокористування,
м. Рівне, Україна
v.v.drozd@nuwm.edu.ua

Ольга Мічута
Національний університет водного господарства та природокористування,
м. Рівне, Україна
o.r.michuta@nuwm.edu.ua

У статті розглядаються проблеми захисту даних в автоматизованих системах управління земельними ресурсами органів місцевого самоврядування в умовах воєнного стану в Україні. Акцент зроблено на необхідності інтеграції сучасних міжнародних стандартів кіберзахисту, зокрема NIST Cybersecurity Framework (CSF) 2.0, у практику місцевих рад для підвищення прозорості та безпеки кадастрових даних. Автор пропонує створення прототипу плагіна для QGIS, який реалізує принципи CSF: ідентифікація активів, захист, моніторинг, реагування та відновлення. Впровадження такого інструменту дозволить знизити ризики маніпуляцій із земельними ресурсами, забезпечити відповідність міжнародним стандартам управління ризиками та підвищити довіру громадян до цифрових сервісів органів влади. [1]

Ключові слова: земельні ресурси; автоматизовані системи; кіберзахист; NIST Cybersecurity Framework (CSF) 2.0; QGIS; місцеве самоврядування; кадастр; воєнний стан

Автоматизовані системи управління земельними ресурсами місцевого самоврядування це геоінформаційні системи, які у своєму складі мають бази даних, що містять певну інформацію з різноманітних реєстрів, зокрема персональні дані. В теперішній час, особливо в умовах воєнного стану, захист інформації від крадіжок, хакерських атак набуває обов'язкового значення. Законодавча база, щодо захисту інформації ґрунтується на Законах України "Про інформацію", "Про доступ до публічної інформації", "Про державну таємницю", "Про захист інформації в інформаційно-комунікаційних системах", "Про електронні комунікації", "Про основні засади забезпечення кібербезпеки України", Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 року № 1229, Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою Кабінет Міністрів України від 29 березня 2006 року № 373 (останні зміни 28 березня 2025 року). Адміністрацією Держспецзв'язку видано наказ від 30 січня 2025 року № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту». Методичні рекомендації щодо здійснення базових заходів з кіберзахисту розроблено з урахуванням документа NIST Cybersecurity Framework (CSF) 2, виданого у 2024 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology). [1]

Фреймворк NIST Cybersecurity Framework (CSF) 2.0 надає універсальний підхід для оцінки та зниження кіберризиків у сфері автоматизації земельних ресурсів. У контексті місцевого самоврядування впровадження CSF дозволяє місцевим радам гарантувати прозорість та достовірність кадастрових даних, знизити ризики махінацій із землею, захистити дані від кібератак та внутрішніх загроз, підвищити довіру громадян до цифрових сервісів. Створення прототипу плагіна для QGIS на основі NIST CSF 2.0 автоматизує моніторинг, захист та аудит дій користувачів у системі. [2; 3; 4]

Розглянемо основні модулі плагіна.

Модуль ідентифікації активів (Identify): автоматично створює інвентаризацію шарів (земельні ділянки, власники, кадастрові номери), визначає критичні дані (наприклад, права власності чи земельні межі).

Модуль контролю доступу (Protect): інтеграція з базою користувачів (LDAP / Active Directory), розмежування доступу (адміністратор, землевпорядник, перегляд для громадян), двофакторна автентифікація при вході.

Модуль моніторингу (Detect): відстеження змін у кадастровій базі в реальному часі, виявлення аномалій (наприклад, якщо площа ділянки зменшена/збільшена >10% без пояснення), журнал змін із можливістю відкату.

Модуль реагування (Respond): автоматичне сповіщення адміністратора про підозрілі зміни, генерація звіту про інцидент, тимчасове блокування підозрілих користувачів.

Модуль відновлення (Recover): інтеграція з системою резервного копіювання, автоматичне відновлення останньої коректної версії шару, перевірка цілісності резервних даних.

Інтерфейс користувача можна представити панель «CyberSecurity Dashboard» у QGIS з 3 вкладками:

Assets & Risks – інвентаризація шарів і ризиків.

Events Monitor – журнал подій і виявлені аномалії.

Recovery – управління резервними копіями та відновленням.

Очікуваний ефект від застосування плагіна полягає у зниженні ризику маніпуляцій із кадастровими даними, підвищенню прозорості діяльності земельного відділу, відповідність міжнародним стандартам управління ризиками, можливість масштабування плагіна для використання в усіх громадах України. [1; 5]

Література.

[1] National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper (CSWP 29). Gaithersburg, MD: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

[2] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. Gaithersburg, MD: NIST, 2020.

[3] Zhiltsov, S., Korytnyi, M., & Malakhov, O. *GIS Technologies for Land Use and Cadastral Systems*. Journal of Geodesy and Cartography, 2021, 45(3), 25–33.

[4] Goodchild, M. F. *GIS and Public Policy: Using Geographic Information Systems for Government Decision-Making*. Annual Review of Public Policy, 2020, 12, 221–240.

[5] European Union Agency for Cybersecurity (ENISA). *Good Practices for Security of IoT and Smart Infrastructure*. ENISA Report, 2021.