Секція С1 Економіка	
УДК 630*6:004.056:330.15	
Дата першого надходження статті до видання	2026-04-21
Дата прийняття статті до друку після рецензування	2026-05-25
Дата публікації/оприлюднення	2026-05-25

ЦИФРОВА БЕЗПЕКА ЛІСОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ЕКОНОМІЧНІ ТА ЕКОЛОГІЧНІ РИЗИКИ

Волковський Юрій Сергійович
аспірант кафедри економіки, туризму та рекреації,
Національний лісотехнічний університет України, вул. Ген. Чупринки,103,
79057, Львів, Україна,
e-mail: volkovskyy.yuriy@nltu.lviv.ua
https://orcid.org/0009-0009-9233-6508

Волковська Юлія Ігорівна
доктор філософії (економіка),
асистентка кафедри економіки, туризму та рекреації.
Національний лісотехнічний університет України, вул. Ген. Чупринки,103,
79057, Львів, Україна,
e-mail: volkovska.yuliia@nltu.edu.ua
https://orcid.org/0000-0002-2594-8864

Анотація. У статті досліджено проблематику цифрової безпеки лісових інформаційних систем (Forest Information Systems, FIS) у контексті зростаючої цифровізації лісового сектору та посилення кліматичних викликів. Метою дослідження є обґрунтування пріоритетних напрямів забезпечення цифрової стійкості лісового сектору України на основі систематизації економічних та екологічних ризиків та наслідків кіберзагроз для лісових інформаційних систем.

Обґрунтовано, що сучасні FIS, які інтегрують дані супутникового моніторингу, геоінформаційних систем, національних інвентаризацій, електронного обліку деревини та платформ раннього виявлення пожеж, перетворилися на критично важливу інфраструктуру управління лісовими ресурсами. Виявлено, що поряд із зростанням ефективності управління лісовим господарством цифровізація створює новий спектр кіберзагроз, реалізація яких може спричиняти системні економічні втрати (зрив роботи аукціонів, спотворення обліку, ризик втрати міжнародних сертифікатів FSC/PEFC) та значні екологічні наслідки (некоректний моніторинг пожеж, ускладнений контроль незаконних рубок, неточність даних щодо вуглецевого балансу).

Встановлено, що порушення цифрової безпеки FIS прямо впливає на виконання Україною вимог EUDR, які набирають чинності 30 грудня 2026 року та на національну звітність у секторі землекористування, змін у землекористуванні та лісового господарства (LULUCF). Систематизовано основні групи кіберризиків та запропоновано пріоритетні напрями забезпечення цифрової стійкості лісового сектору України з урахуванням європейського досвіду та вимог стандарту ISO/IEC 27001. Наукова новизна дослідження полягає у систематизації цифрових загроз для FIS та обґрунтуванні їх впливу на економічну ефективність лісового сектору, достовірність екологічного моніторингу й прийняття управлінських рішень у сфері сталого ведення лісового господарства.

e-ISSN: 2786-586X

Ключові слова: лісові інформаційні системи, цифрова безпека, кіберзагрози, електронний облік деревини, екологічні ризики, економічні наслідки, стале ведення лісового господарства, цифрова стійкість, цифровізація лісового господарства, управління лісовим господарством, моніторинг лісів, лісові екосистеми

DIGITAL SECURITY OF FOREST INFORMATION SYSTEMS: ECONOMIC AND ENVIRONMENTAL RISKS

Yuriy Volkovskyi
PhD Student of the Department of Economics, Tourism and Recreation,
Ukrainian National Forestry University,
103 Gen. Chuprynky St.,
79057, Lviv, Ukraine.
e-mail: volkovskyy.yuriy@nltu.lviv.ua
https://orcid.org/0009-0009-9233-6508

Yuliia Volkovska
PhD in Economics,
Assistant Professor at the Department of Economics, Tourism and Recreation,
Ukrainian National Forestry University,
103 Gen. Chuprynky St.,
79057, Lviv, Ukraine.
e-mail: volkovska.yuliia@nltu.edu.ua
https://orcid.org/0000-0002-2594-8864

Abstract. The article examines the issues of digital security of Forest Information Systems (FIS) in the context of the increasing digitalization of the forestry sector and the intensification of climate-related challenges. The purpose of the study is to substantiate the priority directions for ensuring the digital resilience of the forest sector of Ukraine through the systematization of economic and environmental risks and the consequences of cyber threats for forest information systems.

It is substantiated that modern FIS, which integrate data from satellite monitoring, geographic information systems, national inventories, electronic timber accounting and early fire detection platforms, have become a critically important infrastructure for forest resource management. The study reveals that along with the increase in the efficiency of forest management, digitalization creates a new spectrum of cyber threats, the implementation of which can cause systemic economic losses (disruption of auctions, distortion of accounting, risk of loss of international FSC/PEFC certificates) as well as significant environmental consequences (incorrect fire monitoring, complicated control of illegal logging, inaccuracy of data on the carbon balance).

It was found that a breach of FIS digital security directly affects Ukraine's implementation of the EUDR requirements, which enter into force on December 30, 2026, and on national reporting in the Land Use, Land-Use Change and Forestry (LULUCF) sector. The main groups of cyber risks are systematized and priority areas for ensuring the digital sustainability of the Ukrainian forest sector are proposed, taking into account European experience and the requirements of the ISO/IEC 27001 standard. The scientific novelty of the study lies in the systematization of digital threats to FIS and substantiation of their impact on the economic efficiency of the forest sector, the reliability of environmental monitoring and management decision-making in the field of sustainable forest management.

e-ISSN: 2786-586X

Keywords: forest information systems, digital security, cyber threats, electronic timber accounting, environmental risks, economic consequences, sustainable forest management, digital resilience, digitalization of forestry, forest governance, forest monitoring, forest ecosystems.

Вступ

Актуальність проблеми. Глобальні процеси цифровізації істотно змінюють підходи до управління природними ресурсами. Лісовий сектор не є винятком: на національному й міжнародному рівнях упроваджуються комплексні цифрові платформи, які перетворюють спосіб збору, зберігання та використання даних про ліси. Лісові інформаційні системи (Forest Information Systems, FIS) сьогодні поєднують засоби супутникового моніторингу, геоінформаційні системи (GIS), електронний облік деревини, системи раннього виявлення пожеж, національні інвентаризації та платформи відкритих даних. Ці інструменти забезпечують прозорість та оперативність прийняття рішень, а також виконання міжнародних кліматичних зобов'язань.

Водночас зростання цифрової залежності лісового сектору формує принципово новий вимір ризиків в лісовому господарстві, яким є кіберзагрози. Якщо традиційно безпека лісів асоціювалася з протипожежним захистом, охороною від незаконних рубок та фітосанітарним контролем, то нині безпека лісових даних стає не менш значущим аспектом сталого управління лісовим господарством. Будь-яке порушення цілісності, доступності або достовірності інформації у FIS здатне трансформуватися у відчутні економічні втрати та екологічні наслідки. Особливої актуальності проблема набуває для України, де в умовах воєнних викликів та підготовки до європейської інтеграції цифрова інфраструктура лісового сектору стає одночасно ключовим інструментом ефективності управління лісовим господарством, а також потенційною мішенню для зловмисників.

У сучасній науковій літературі та практиці ведення лісового господарства проблематика цифрової безпеки FIS залишається недостатньо опрацьованою. Переважна більшість досліджень фокусується на технологічних аспектах цифровізації (впровадженні дистанційного зондування, IoT-сенсорів, систем електронного обліку), тоді як питання захисту даних, безперервності роботи сервісів та оцінки еколого-економічних наслідків кіберінцидентів розглядаються частково. Зважаючи на зростаючу взаємозалежність національних та міжнародних систем (EFFIS, Copernicus, EUDR-платформи), виникає об'єктивна потреба у системному аналізі ризиків цифрової безпеки FIS та формуванні комплексних підходів до їх мінімізації з урахуванням специфіки лісового сектору.

Аналіз останніх досліджень і публікацій. Теоретичні та прикладні аспекти подальшого розвитку та застосування лісових інформаційних систем активно досліджуються міжнародними організаціями. Так, у Посібнику зі створення ефективних ЛІС Європейської економічної комісії ООН (UNECE) [1], ці системи розглядаються як інструмент підтримки лісової політики, управління ресурсами, моніторингу результатів і комунікації між зацікавленими сторонами. Окремо наголошується про залежність структури такої системи від потреб окремо взятої країни, внутрішнього законодавства, адміністративної та управлінської систем.

Цифрова трансформація лісового сектору в межах переходу до концепції FOREST 4.0 (або "Лісове господарство 4.0") охоплює застосування технологій на основні ШІ (штучного інтелекту) та IoT (Інтернету речей) для вдосконалення моніторингу стану лісів, збору та обробки відповідних даних [2,3]. У своєму дослідженні Damaševičius R. et al. [4] наголошують, що цифровізація лісового сектору розширює можливості моніторингу та управління, але водночас створює нові вимоги до захисту даних, цифрової інфраструктури та довіри до технологічних рішень.

e-ISSN: 2786-586X

F. M. Gültekin, та ін [5] досліджують застосування великих мовних моделей для оцінювання кіберризиків у цифровізованих системах лісового господарства Forestry 4.0, зосереджуючись на підвищенні стійкості цифрової інфраструктури та зменшенні можливих економічних втрат від кіберінцидентів. Водночас, M. Mohamad та ін [6] аналізують питання кібербезпеки сучасної лісозаготівельної техніки, зокрема вимоги європейської сертифікації щодо безпеки та відповідності технічним стандартам, безпечної експлуатації та інтеграції технологій штучного інтелекту в цифрові системи управління лісовим господарством.

Дослідження питання цифровізації ланцюгів постачання деревини [7] та застосування технологій блокчейну [8] для управління лісовим господарством, простежування лісопродукції та виявлення лісових пожеж підкреслюють вплив цифрових даних на економічну ефективність лісового сектору. Блокчейн-технології розглядаються як один із потенційних інструментів підвищення прозорості та простежуваності ланцюгів постачання деревини в умовах вимог EUDR [9].

Водночас у галузевих аналітичних матеріалах V. S. Maddela [10] акцентує увагу на зростанні кіберризиків у секторі торгівлі деревиною та продуктами її переробки, зокрема ризиках порушення цифрових ланцюгів постачання, витоку даних і пов'язаних із цим економічних та репутаційних втрат.

Питання захисту інформаційних ресурсів та цифрової інфраструктури лісового сектору також відображені у директиві Лісової служби США "6680 - Cybersecurity of Information, Information Systems, and Information Technology" [11], яка встановлює вимоги до кіберзахисту інформації, інформаційних систем та IT-ресурсів лісового відомства.

В Україні цифрові рішення у лісовому секторі сьогодні переважно пов'язані з електронним обліком деревини, GIS-моніторингом та автоматизацією управління лісовими ресурсами. Водночас питання цифрової безпеки лісових інформаційних систем, стійкості цифрової інфраструктури та наслідків кіберінцидентів для економічної й екологічної безпеки галузі поки залишаються малодослідженими. У таких умовах впровадження ДП «Лісогосподарський Інноваційно-Аналітичний Центр» системи управління інформаційною безпекою відповідно до ISO/IEC 27001:2022 свідчить про поступове включення питань кібербезпеки до практики управління лісовим сектором України [12].

Мета статті. Метою статті є комплексний аналіз цифрової безпеки лісових інформаційних систем, систематизація економічних та екологічних ризиків і наслідків, пов'язаних із кіберзагрозами для FIS, а також обґрунтування пріоритетних напрямів забезпечення цифрової стійкості лісового сектору України з урахуванням європейського досвіду.

Основні результати. Лісові інформаційні системи (FIS) - це комплекс цифрових платформ та інструментів, які забезпечують збирання, зберігання, обробку, поширення та аналітичне використання даних про ліси. У міжнародній практиці сучасні FIS мають комплексну структуру та поєднують інструменти дистанційного зондування, геоінформаційного аналізу, цифрового моніторингу, електронного обліку деревини та систем підтримки управлінських рішень [13].

Важливу роль у функціонуванні FIS відіграють підсистеми дистанційного зондування та супутникового моніторингу, які використовують дані супутників Sentinel та Landsat для виявлення пожеж, змін лісового покриву, всихання насаджень та моніторингу деградації в умовах кліматичних змін [14]. Геоінформаційні системи (GIS) забезпечують створення й ведення цифрових карт лісів, просторовий аналіз стану насаджень та моделювання ризиків, пов'язаних з лісовими пожежами, ерозієї грунтів та поширенням шкідників.

e-ISSN: 2786-586X

Важливим елементом FIS є національні системи інвентаризації лісів (NFI/NFMS), які використовуються для вимірювання площ, запасів, віку та категорій лісів, формування національних кліматичних звітів у межах LULUCF та відстеження довгострокових змін структури лісових екосистем [15]. Окремий напрям становлять системи електронного обліку та простежуваності деревини, що включають електронний облік деревини (ЕОД) для маркування та руху деревини, онлайн-формування лісорубних квитків і накладних та контроль легальності походження відповідно до стандартів FSC/PEFC і регламенту EUDR.

Сучасні FIS також інтегрують спеціалізовані платформи пожежного моніторингу та раннього виявлення ризиків, зокрема European Forest Fire Information System (EFFIS), за допомогою яких відбувається відстеження лісових пожеж, моделювання поширення вогню та фіксація наслідків [16]. Додатковим елементом є системи відкритих даних і публічні інформаційні портали, які забезпечують прозорість та доступ громадськості до інформації про стан лісових екосистем.

Така структура FIS одночасно розширює можливості управління лісовим сектором, але, водночас, і підвищує його залежність від стабільності роботи цифрової інфраструктури та достовірності отриманих даних. У зв'язку з цим особливої актуальності набувають питання цифрової безпеки та основних кіберзагроз для FIS. Класифікація цифрових загроз для лісових інформаційних систем є важливою передумовою оцінювання потенційних економічних та екологічних ризиків, пов'язаних із функціонуванням цифрової інфраструктури лісового сектору.

Проаналізувавши основі цифрова загрози для FIS, пропонуємо виділити такі основні групи:

1. Ризики фальсифікації або викривлення даних у системах електронного обліку та простежуваності деревини, націлені на легалізацію незаконних вирубок та маніпуляції з сертифікацією. Для України це має безпосереднє практичне значення, оскільки Єдина державна система електронного обліку деревини забезпечує фіксацію місця заготівлі, характеристик і переміщення деревини та використовується для підтвердження її походження. Відсутність відповідних даних у системі унеможливлює належне підтвердження легальності походження деревини та її простежуваності [17].

2. Порушення доступності цифрових сервісів та інфраструктури. Функціонування сучасних FIS залежить від стабільної роботи серверів, цифрових платформ, супутникових каналів зв'язку та систем передавання даних. Особливе значення це має для платформ пожежного моніторингу та раннього виявлення пожежних ризиків. Зокрема, European Forest Fire Information System (EFFIS) забезпечує оперативну інформацію про пожежну небезпеку, активні пожежі та оцінювання їх наслідків [16]. Відповідно, збої цифрової інфраструктури або затримка передавання даних можуть безпосередньо впливати на ефективність реагування та масштаби екологічних і економічних збитків. У документах FAO та IPCC також підкреслюється критична роль достовірних даних для систем моніторингу лісів, оцінювання вуглецевого балансу та формування кліматичної звітності у межах LULUCF.

3. Несанкціонований доступ та порушення управління правами користувачів. Лісові інформаційні системи містять значні масиви стратегічних даних, зокрема результати лісових інвентаризацій, кліматичної звітності, геопросторового моніторингу та аналітичних моделей. Недостатній контроль доступу, витоки даних або компрометація облікових записів можуть створювати як економічні, так і управлінські ризики для лісового сектору. У міжнародній практиці для мінімізації таких ризиків застосовуються системи Privileged Access Management (PAM), які забезпечують контроль привілейованого доступу до критичної цифрової інфраструктури та баз даних [18].

Цифрові загрози для лісових інформаційних систем мають комплексний характер, оскільки порушення цілісності даних, доступності цифрових сервісів або безпеки

e-ISSN: 2786-586X

цифрової інфраструктури здатне впливати не лише на функціонування FIS, але й на економічні показники лісового сектору, процеси екологічного моніторингу та виконання кліматичних зобов'язань. Особливого значення це набуває у контексті вимог EUDR та формування національної звітності у секторі землекористування, змін у землекористуванні та лісового господарства (LULUCF). З огляду на це доцільно розглянути основні економічні та екологічні наслідки цифрових загроз для лісових інформаційних систем (табл. 1).

Таблиця 1. Систематизація економічних та екологічних наслідків реалізації кіберзагроз для лісових інформаційних систем

№	Тип наслідку	Механізм реалізації
	Економічні наслідки	
1	Призупинення роботи систем обліку та електронних аукціонів	Зрив оформлення дозвільних документів і реалізації деревини; розширення можливостей для тіньових операцій
2	Порушення цифрової логістики деревини	Збій електронного лісорубного квитка, електронних товарно-транспортних накладних з фотофіксацією та GPS-моніторингу спецтехніки
3	Ризик блокування експорту до ЄС	Невідповідність вимогам EUDR щодо геолокаційної простежуваності деревини у разі порушення цілісності даних
4	Втрата сертифікацій FSC / PEFC	Порушення цілісності даних у рішеннях класу TimberID, які забезпечують Due Diligence Statement та селективне оприлюднення документів
5	Зростання транзакційних витрат на відновлення	Витрати на відновлення інфраструктури FIS, проведення аудиту достовірності даних, репутаційні втрати
	Екологічні наслідки	
6	Зниження ефективності протидії пожежам	Зниження якості та своєчасності даних EFFIS у пожежонебезпечний сезон; часткове пом'якшення завдяки IoT-фреймворкам і дрон-IoT-системам раннього виявлення
7	Погіршення контролю за незаконними рубками	Нездатність національних систем відстеження виявляти порушення без верифікації обсягів при першому розміщенні деревини на ринку; перспективне використання смарт-контрактів блокчейну
8	Викривлення показників сталого ведення лісового господарства	Погіршення якості просторового моніторингу та геолокаційної простежуваності; залежність від інтеграції даних Copernicus Sentinel-2 та алгоритмів машинного навчання
9	Неправильне планування рубок і лісовідновлення	Прийняття управлінських рішень щодо рубок та відновлення лісового покриву на основі неточних карт і викривлених вхідних даних

e-ISSN: 2786-586X

№	Тип наслідку	Механізм реалізації
10	Порушення оцінки вуглецевого балансу	Спотворення показників поглинання й емісій парникових газів у секторі LULUCF; вплив на національну кліматичну звітність перед Рамковою конвенцією ООН

Джерело: узагальнено авторами на основі [21-24,27-29]

Систематизація економічних та екологічних наслідків кіберзагроз для лісових інформаційних систем, представлена у таблиці 1, демонструє каскадний характер їх реалізації. Економічна група наслідків (позиції 1-5) формується переважно у короткостроковій перспективі та виявляється через зрив операційних процесів цифрової інфраструктури лісового сектору. Перші два наслідки пов'язані зі статистикою незаконних рубок в Україні, обсяг яких становив 703,9 млн грн у 2023 році та 697 млн грн за дев'ять місяців 2025 року [19, 20]. Третій і четвертий наслідки пов'язані з виконанням вимог Регламенту (ЄС) 2023/1115 (EUDR), які для великих операторів стають обов'язковими з 30 грудня 2026 року [21, 22].

Екологічна група наслідків (позиції 6-10) має відтермінований і часто незворотний характер. Зниження ефективності протидії лісовим пожежам в Європі оцінюється щорічно у близько 65 тис. лісових пожеж із сукупною площею ураження приблизно 0,5 млн га, причому понад 85 % згорілих площ припадає на Середземноморський регіон [23]. Неправильне планування рубок та порушення оцінки вуглецевого балансу проявляються у довгостроковому горизонті через каскадний ефект від похибок у вхідних даних просторового моніторингу до національної кліматичної звітності у секторі LULUCF згідно з регламентами IPCC [24]. Таким чином, кожний кіберінцидент у FIS потенційно трансформується з технічного збою у комплексну економіко-екологічну подію, що актуалізує потребу у пріоритетному впровадженні системи управління інформаційною безпекою на основі ISO/IEC 27001:2022.

Україна досягла суттєвого прогресу у цифровізації лісового сектору. Єдина державна система електронного обліку деревини (ЕОД) забезпечує цифровий контроль руху деревини в режимі реального часу. У лісовому секторі також функціонують Єдиний реєстр лісорубних квитків, сервіси перевірки походження деревини, GPS-моніторинг спеціалізованої техніки, електронний контроль транспортування деревини та системи фотофіксації транспортних засобів. Окремим напрямом цифровізації є використання спеціалізованої автоматизованої системи «Пожежі» для моніторингу пожежної ситуації. Розвиток таких цифрових інструментів свідчить про посилення контролю за використанням лісових ресурсів, простежуваністю лісопродукції та моніторингом стану лісового фонду.

У сфері захисту цих систем ДП «ЛІАЦ» реалізує багаторівневу модель безпеки, що включає захищені мережі та обмеження доступу, постійний моніторинг кіберзагроз, двофакторну автентифікацію (2FA) для всіх користувачів ЕОД та аудит дій. Розроблено внутрішні документи з регламентації дій у кризових ситуаціях, включно з планом реагування на надзвичайні ситуації та порядком резервного копіювання інформації. Ключові системи зберігаються на фізичних серверах, у хмарних сховищах та на резервних потужностях за кордоном, що забезпечує їх безперебійну роботу навіть у воєнних умовах [12, 25]. У жовтні 2025 року ДП «ЛІАЦ» оголосило про початок упровадження системи управління інформаційною безпекою (СУІБ) із сертифікацією відповідно до міжнародного стандарту ISO/IEC 27001:2022 [26].

На основі аналізу міжнародного досвіду та оцінки наявного стану цифрової безпеки лісового сектору України можна виокремити наступні пріоритетні напрями її подальшого розвитку. Завершення сертифікації за ISO/IEC 27001:2022 та

e-ISSN: 2786-586X

розповсюдження стандарту на всіх ключових операторів лісового сектору сприятиме інституціоналізації системи управління інформаційною безпекою (ISMS). Іноземним орієнтиром тут є практика Служби лісу США, що має окрему главу ForestService Handbook щодо кібербезпеки. Наступний критичний напрям - поглиблення політики управління доступом за принципом Privileged Access Management (PAM), яка регулює та контролює привілейовані облікові записи, забезпечуючи доступ до чутливих систем лише уповноваженому персоналу. Також потрібно звернути увагу на посилення механізмів резервування даних, географічно розподілене зберігання та регулярне тестування процедур відновлення. Впровадження систем виявлення аномалій на базі алгоритмів машинного навчання сприятиме швидкому аналізу журналів доступу, зміни даних і мережевого трафіку для виявлення підозрілої поведінки. Слід зауважити, що підготовка кваліфікованих кадрів у сфері кіберзахисту лісового сектору, що передбачає міждисциплінарну освіту на стику лісотехнічних, ІТ- та безпекових дисциплін, а також періодичне підвищення кваліфікації працівників лісогосподарських підприємств є вкрай важливим аспектом розвитку цифрової безпеки FIS. Реалізація цих напрямів дозволить інтегрувати цифрову безпеку в загальну стратегію сталого ведення лісового господарства і забезпечити стійкість сектору в умовах гібридних загроз і кліматичних викликів.

Висновки

Лісові інформаційні системи перетворилися на критично важливу інфраструктуру управління лісовими ресурсами та виконання міжнародних кліматичних зобов'язань. Їх цілісність, доступність та достовірність даних безпосередньо впливають на якість екологічних рішень та економічну стійкість лісового сектору, а вразливість цифрових компонентів стає системним ризиком національного й транснаціонального рівня.

Цифрові загрози для FIS формують п'ять основних груп ризиків - підміну й фальсифікацію даних, виведення з ладу систем раннього виявлення пожеж, маніпуляції логістичними системами, кібершпигунство та вплив на моделі екосистемних сервісів. Реалізація цих загроз має каскадний характер, коли технічний інцидент породжує економічні втрати, які своєю чергою трансформуються в екологічні наслідки.

Економічні наслідки кіберінцидентів проявляються через зрив роботи аукціонів та систем обліку, порушення логістичних ланцюгів, зростання витрат на відновлення інфраструктури, втрату довіри міжнародних партнерів та ризик втрати сертифікацій FSC/PEFC і блокування експорту відповідно до вимог EUDR. Екологічні наслідки мають відстрочений і часто незворотний характер: збільшення площ пожеж, спотворення обліку рубок, погіршення якості моніторингу деградації, неточність даних щодо вуглецевого балансу та загрози біорізноманіттю.

Україна досягла значних результатів у цифровізації лісового сектору (ЕОД, фотофіксація, GPS-моніторинг, відкриті дані), а ДП «ЛІАЦ» закладає основи системного кіберзахисту через двофакторну автентифікацію, географічне резервування даних та плановану сертифікацію за ISO/IEC 27001:2022.

Стратегічними напрямами модернізації цифрової безпеки FIS в Україні є завершення впровадження ISMS на основі ISO/IEC 27001, поглиблення політики управління привілейованим доступом, посилення резервування даних, інтеграція алгоритмів виявлення аномалій та підготовка профільних кадрів. Поєднання цифровізації та кіберзахисту є необхідною умовою сталого розвитку лісового сектору, особливо в умовах війни та підготовки до європейської інтеграції.

Список використаних джерел

1. UNECE. Developing Forest Information Systems: A Guide to Creating Effective Forest Information Systems. URL:

e-ISSN: 2786-586X

https://www.zemeunvalsts.lv/documents/view/bc9c8c705927bf419147ab7491c54896/UNECE%20Developing%20Forest%20Information%20Systems%202026.pdf
2. Centre of Excellence to Transform the Forest Environment Monitoring. URL: https://forest40.lt/
3. Singh R., Gehlot A., Akram S.V., Thakur A.K., Buddhi D., Das P.K. Forest 4.0: Digitalization of Forest Using the Internet of Things (IoT). Journal of King Saud University - Computer and Information Sciences. 2021. URL: https://www.sciencedirect.com/science/article/pii/S1319157821000483
4. Damaševičius R., Mozgeris G., Kurti A., Maskeliūnas R. Digital Transformation of the Future of Forestry: An Exploration of Key Concepts in the Principles Behind Forest 4.0. Frontiers in Forests and Global Change. 2024. Vol. 7. Article 1424327. DOI: https://doi.org/10.3389/ffgc.2024.1424327
5. Gültekin F.M., Lilja O., Khojah R., Wohlrab R., Damschen M., Mohamad M. Leveraging Large Language Models for Cybersecurity Risk Assessment - A Case from Forestry Cyber-Physical Systems. arXiv Preprint. 2025. DOI: https://doi.org/10.48550/arXiv.2510.06343
6. Mohamad M., Avula R.R., Folkesson P., Kleberger P., Mirzai A., Skoglund M., Damschen M. Cybersecurity Pathways Towards CE-Certified Autonomous Forestry Machines. 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Brisbane, Australia, 2024. DOI: https://doi.org/10.48550/arXiv.2404.19643
7. Palander T., Tokola T., Borz S.A. et al. Forest Supply Chains During Digitalization: Current Implementations and Prospects in Near Future. Current Forestry Reports. 2024. Vol. 10. P. 223–238. DOI: https://doi.org/10.1007/s40725-024-00218-4
8. He Z., Turner P. Blockchain Applications in Forestry: A Systematic Literature Review. Applied Sciences. 2022. Vol. 12, No. 8. Article 3723. DOI: https://doi.org/10.3390/app12083723
9. Forest Information System of Europe. Timber Traceability: Pioneering Innovation to Eradicate Deforestation from Europe's Supply Chain. EEA, 2024. URL: https://forest.eea.europa.eu/resources/research-corner/research-highlights/timber-traceability-pioneering-innovation-to-eradicate-deforestation-from-europes-supply-chain
10. Maddela V.S. Cyber Insecurity: Safeguarding the Timber and Wood Products Trade Industry. Timber Trades Journal. 2024. URL: https://www.ttjonline.com/risks/navigating-cyber-insecurity-safeguarding-the-timber-and-wood-products-trade-industry/
11. USDA Forest Service. Manual 6600 System Management 6680 Cybersecurity of Information, Information Systems, and Information Technology. URL: https://www.usda.gov/guidance-documents/cybersecurity-information-information-systems-and-information-technology/fs/forestservicemanual-6600-system-management-6680-cybersecurity-information-information-systems-and
12. Держлісагентство. Захист за міжнародним стандартом: ДП «ЛІАЦ» впроваджує систему управління інформаційною безпекою. 2025. URL: https://forest.gov.ua/news/zakhyst-za-mizhnarodnym-standartom-dp-liats-vprovadzhuie-systemu-upravlinnia-informatsiinoiu-bezpekoiu
13. UNECE. Developing National Forest Information Systems: A Practical Guide. URL: https://unece.org/sites/default/files/202601/2326210_E_ECE_TIM_SP_56_WEB.pdf
14. FAO. FRA 2020 Remote Sensing Survey. URL: https://www.fao.org/forest-resources-assessment/remote-sensing/remote-sensing-survey/en
15. FAO. National Forest Monitoring Systems. URL: https://www.fao.org/redd/areas-of-work/national-forest-monitoring-system/en
16. EFFIS. European Forest Fire Information System. Joint Research Centre, European Commission. URL: https://effis.emergency.copernicus.eu/
17. Держлісагентство. Всі лісокористувачі відтепер зобов'язані користуватися системою електронного обліку деревини. 2021. URL: https://forest.gov.ua/news/vsi-

e-ISSN: 2786-586X

lisokoristuvachi-vidteper-zobovyazani-koristuvatisya-sistemoyu-elektronnogo-obliku-derevini

18. SSH Communications Security. Securing Forestry Industry Control Systems with PrivX Hybrid PAM. URL: https://www.ssh.com/academy/pam/securing-forestry-industry-control-systems-with-privx-hybrid-pam
19. Інтерфакс-Україна. Глава Мінекономіки анонсував запровадження повного цифрового контролю за лісозаготівлею. URL: https://interfax.com.ua/news/economic/1133266.html (дата звернення: 15.05.2026).
20. Незаконні рубки деревини в Україні: яка область очолює антирекорд. URL: https://eco.rayon.in.ua/news/755743-nezakonni-rubki-derevini-v-ukraini-yaka-oblast-ocholyue-antirekord (дата звернення: 15.05.2026).
21. Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the Making Available on the Union Market and the Export from the Union of Certain Commodities and Products Associated with Deforestation and Forest Degradation and Repealing Regulation (EU) No 995/2010. Official Journal of the European Union. 2023. L 150. P. 206–247. URL:https://eurlex.europa.eu/eli/reg/2023/1115/oj
22. PEFC. The TimberID Supply Chain Solution to Ensure EUDR Compliance. Programme for the Endorsement of Forest Certification, 2024. URL: https://pefc.org/cms/b999fadb-8521-4d4f-8d3c-4688f57fdced/news/10001145/the-timberid-supply-chain-solution-to-ensure-eudr-compliance (дата звернення: 15.05.2026).
23. Ramadan M.N.A. та ін. Towards Early Forest Fire Detection and Prevention Using AI-Powered Drones and the IoT. Internet of Things. 2024. Vol. 27. Article 101248. DOI: https://doi.org/10.1016/j.iot.2024.101248
24. IPCC. 2019 Refinement to the 2006 IPCC Guidelines for National Greenhouse Gas Inventories. Volume 4: Agriculture, Forestry and Other Land Use (AFOLU). Geneva, 2019.
25. Держлісагентство. Захист ІТ-інфраструктури лісової галузі: як убезпечують роботу інформаційних систем. 2025. URL: https://forest.gov.ua/news/zakhyst-it-infrastruktury-lisovoi-haluzi-iak-ubezpechuiut-robotu-informatsiinykh-system
26. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. International Organization for Standardization, 2022. URL: https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf
27. Остапчук С., Дриманова Л., Бараненко Ю. Електронний облік продукції лісового господарства в Україні: проблеми та шляхи вдосконалення. Облік і фінанси. 2023. № 4 (102). С. 26–38. DOI: https://doi.org/10.33146/2307-9878-2023-4(102)-26-38
28. San-Miguel-Ayanz J., Schulte E., Schmuck G., Camia A., Strobl P., Liberta G., Giovando C., Boca R., Sedano F., Kempeneers P., McInerney D., Withmore C., Santos de Oliveira S., Rodrigues M., Durrant T., Corti P., Oehler F., Vilar L., Amatulli G. Comprehensive Monitoring of Wildfires in Europe: The European Forest Fire Information System (EFFIS). Approaches to Managing Disaster - Assessing Hazards, Emergencies and Disaster Impacts. InTech, 2012. DOI: https://doi.org/10.5772/28441
29. Etaati E. та ін. Smart Forest Monitoring: A Novel Internet of Things Framework with Shortest Path Routing for Sustainable Environmental Management. IET Networks. 2024. Vol. 13, No. 5-6. P. 528–545. DOI: https://doi.org/10.1049/ntw2.12135

References

1. UNECE. (2026). Developing Forest Information Systems: A Guide to Creating Effective Forest Information Systems. Retrieved from

e-ISSN: 2786-586X

https://www.zemeunvalsts.lv/documents/view/bc9c8c705927bf419147ab7491c54896/UNECE%20Developing%20Forest%20Information%20Systems%202026.pdf

2. Centre of Excellence to Transform the Forest Environment Monitoring. (n.d.). Retrieved from https://forest40.lt/

3. Singh, R., Gehlot, A., Akram, S. V., Thakur, A. K., Buddhi, D., & Das, P. K. (2021). Forest 4.0: Digitalization of forest using the Internet of Things (IoT). Journal of King Saud University - Computer and Information Sciences. Retrieved from https://www.sciencedirect.com/science/article/pii/S1319157821000483

4. Damaševičius, R., Mozgeris, G., Kurti, A., & Maskeliūnas, R. (2024). Digital transformation of the future of forestry: An exploration of key concepts in the principles behind Forest 4.0. Frontiers in Forests and Global Change, 7, Article 1424327. https://doi.org/10.3389/ffgc.2024.1424327

5. Gültekin, F. M., Lilja, O., Khojah, R., Wohlrab, R., Damschen, M., & Mohamad, M. (2025). Leveraging large language models for cybersecurity risk assessment: A case from forestry cyber-physical systems. arXiv Preprint. https://doi.org/10.48550/arXiv.2510.06343

6. Mohamad, M., Avula, R. R., Folkesson, P., Kleberger, P., Mirzai, A., Skoglund, M., & Damschen, M. (2024). Cybersecurity pathways towards CE-certified autonomous forestry machines. In 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Brisbane, Australia. https://doi.org/10.48550/arXiv.2404.19643

7. Palander, T., Tokola, T., Borz, S. A., et al. (2024). Forest supply chains during digitalization: Current implementations and prospects in near future. Current Forestry Reports, 10, 223–238. https://doi.org/10.1007/s40725-024-00218-4

8. He, Z., & Turner, P. (2022). Blockchain applications in forestry: A systematic literature review. Applied Sciences, 12(8), Article 3723. https://doi.org/10.3390/app12083723

9. Forest Information System of Europe. (2024). Timber traceability: Pioneering innovation to eradicate deforestation from Europe's supply chain. Retrieved from https://forest.eea.europa.eu/resources/research-corner/research-highlights/timber-traceability-pioneering-innovation-to-eradicate-deforestation-from-europes-supply-chain

10. Maddela, V. S. (2024). Cyber insecurity: Safeguarding the timber and wood products trade industry. Timber Trades Journal. Retrieved from https://www.ttjonline.com/risks/navigating-cyber-insecurity-safeguarding-the-timber-and-wood-products-trade-industry/

11. USDA Forest Service. (n.d.). Manual 6600 System Management 6680 Cybersecurity of Information, Information Systems, and Information Technology. Retrieved from https://www.usda.gov/guidance-documents/cybersecurity-information-information-systems-and-information-technology/fs/forestservicemanual-6600-system-management-6680-cybersecurity-information-information-systems-and

12. Derzhlisahentstvo. (2025). Zakhyst za mizhnarodnym standartom: DP «LIATs» vprovadzhuie systemu upravlinnia informatsiinoiu bezpekoiu [Protection according to international standards: State Enterprise "LIAC" implements an information security management system]. Retrieved from https://forest.gov.ua/news/zakhyst-za-mizhnarodnym-standartom-dp-liats-vprovadzhuie-systemu-upravlinnia-informatsiinoiu-bezpekoiu

13. UNECE. (2026). Developing National Forest Information Systems: A Practical Guide. Retrieved from https://unece.org/sites/default/files/202601/2326210_E_ECE_TIM_SP_56_WEB.pdf

14. FAO. (2020). FRA 2020 Remote Sensing Survey. Retrieved from https://www.fao.org/forest-resources-assessment/remote-sensing/remote-sensing-survey/en

15. FAO. (n.d.). National Forest Monitoring Systems. Retrieved from https://www.fao.org/redd/areas-of-work/national-forest-monitoring-system/en

e-ISSN: 2786-586X

16. EFFIS. (n.d.). European Forest Fire Information System. Joint Research Centre, European Commission. Retrieved from https://effis.emergency.copernicus.eu/

17. Derzhlisahentstvo. (2021). Vsi lisokorystuvachi vidteper zobov'iazani korystuvatysia systemoiu elektronnoho obliku derevyny [All forest users are now required to use the electronic timber accounting system]. Retrieved from https://forest.gov.ua/news/vsi-lisokoristuvachi-vidteper-zobovyazani-koristuvatisya-sistemoyu-elektronnogo-obliku-derevini

18. SSH Communications Security. (n.d.). Securing forestry industry control systems with PrivX Hybrid PAM. Retrieved from https://www.ssh.com/academy/pam/securing-forestry-industry-control-systems-with-privx-hybrid-pam

19. Interfaks-Ukraina. (2026). Hlava Minekonomiky anonsuvav zaprovadzhennia povnoho tsyfrovoho kontroliu za lisozahotivleiu [The Minister of Economy announced the introduction of full digital control over logging]. Retrieved from https://interfax.com.ua/news/economic/1133266.html

20. Nezakonni rubky derevyny v Ukraini: yaka oblast ocholiuie antyrekord [Illegal logging in Ukraine: Which region leads the anti-record]. (2026). Retrieved from https://eco.rayon.in.ua/news/755743-nezakonni-rubki-derevini-v-ukraini-yaka-oblast-ocholyue-antirekord

21. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1115 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010. Official Journal of the European Union, L150, 206–247. Retrieved from https://eur-lex.europa.eu/eli/reg/2023/1115/oj

22. PEFC. (2024). The TimberID supply chain solution to ensure EUDR compliance. Programme for the Endorsement of Forest Certification. Retrieved from https://pefc.org/cms/b999fadb-8521-4d4f-8d3c-4688f57fdced/news/10001145/the-timberid-supply-chain-solution-to-ensure-eudr-compliance

23. Ramadan, M. N. A., et al. (2024). Towards early forest fire detection and prevention using AI-powered drones and the IoT. Internet of Things, 27, Article 101248. https://doi.org/10.1016/j.iot.2024.101248

24. IPCC. (2019). 2019 Refinement to the 2006 IPCC Guidelines for National Greenhouse Gas Inventories. Volume 4: Agriculture, Forestry and Other Land Use (AFOLU). Geneva.

25. Derzhlisahentstvo. (2025). Zakhyst IT-infrastruktury lisovoi haluzi: yak ubezpechuiut robotu informatsiinykh system [Protection of the IT infrastructure of the forestry sector: How the operation of information systems is secured]. Retrieved from https://forest.gov.ua/news/zakhyst-it-infrastruktury-lisovoi-haluzi-iak-ubezpechuiut-robotu-informatsiinykh-system

26. ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization. Retrieved from https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf

27. Ostapchuk, S., Drymanova, L., & Baranenko, Yu. (2023). Elektronnyi oblik produktsii lisovoho hospodarstva v Ukraini: problemy ta shliakhy vdoskonalennia [Electronic accounting of forestry products in Ukraine: Problems and ways of improvement]. Oblik i Finansy, 4(102), 26–38. https://doi.org/10.33146/2307-9878-2023-4(102)-26-38

28. San-Miguel-Ayanz, J., Schulte, E., Schmuck, G., Camia, A., Strobl, P., Liberta, G., et al. (2012). Comprehensive monitoring of wildfires in Europe: The European Forest Fire Information System (EFFIS). In Approaches to Managing Disaster - Assessing Hazards, Emergencies and Disaster Impacts. InTech. https://doi.org/10.5772/28441

e-ISSN: 2786-586X

29. Etaati, E., et al. (2024). Smart forest monitoring: A novel Internet of Things framework with shortest path routing for sustainable environmental management. IET Networks, 13(5-6), 528–545. https://doi.org/10.1049/ntw2.12135

e-ISSN: 2786-586X