Ковальов К.Є.,
старший науковий співробітник
Українського науково-дослідного
інституту спеціальної техніки та судових експертиз
Служби безпеки України

УДК 342.9
DOI 10.32782/2663-5666.2025.1.12

СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ

Вступ. Критична інфраструктура – це сукупність життєво важливих об'єктів та систем, які забезпечують стабільне функціонування держави, економіки та суспільства. До неї належать енергетичні мережі, транспортні вузли, зв'язок, системи водопостачання, охорона здоров'я, банківська система, оборонна промисловість, а також інформаційні технології. У мирний час критична інфраструктура забезпечує нормальне життя громадян і розвиток держави, але в умовах війни вона стає головною мішенню для ворога.

Останні дослідження та публікації висвітлюють низку актуальних викликів і загроз для критичної інфраструктури України в умовах воєнного стану. Російська агресія призвела до масштабних руйнувань об'єктів критичної інфраструктури України. Зокрема, обстріли та бомбардування пошкодили енергетичні об'єкти, транспортні мережі та промислові підприємства, що негативно вплинуло на економіку та життєзабезпечення населення. Відновлення цих об'єктів потребує комплексного підходу та значних ресурсів.

Критична інфраструктура України зазнає постійних кібернетичних атак, спрямованих на дестабілізацію її функціонування. Особливо вразливими є енергетичні об'єкти, медичні установи та державні інформаційні системи. Використання штучного інтелекту для моніторингу загроз, прогнозування атак та захисту даних стає важливим елементом забезпечення кібербезпеки.

Аналіз нормативно-правової бази України вказує на необхідність вдосконалення державної системи захисту критичної інфраструктури. Розробка та впровадження ефективних механізмів координації дій між державними органами та приватним сектором є ключовими для підвищення стійкості інфраструктури до загроз.

Воєнні дії створюють значні виклики для економічної безпеки України. Руйнування інфраструктури, зниження промислового виробництва та фінансові втрати потребують впровадження стратегій для забезпечення стійкості економіки та швидкого відновлення після завершення конфлікту.

Розробка моделей загроз для критичної інфраструктури дозволяє більш ефективно оцінювати ризики та планувати заходи з їх нейтралізації. Це включає аналіз потенційних сценаріїв атак, вразливостей об'єктів та розробку відповідних заходів реагування.

Узагальнюючи, сучасні дослідження підкреслюють необхідність комплексного підходу до захисту критичної інфраструктури України, що включає фізичну безпеку, кіберзахист, нормативно-правове забезпечення та економічну стійкість.

Аналіз літературних джерел з теми відображає різноманітні підходи та дослідження в цій сфері. Такі науковці, як Охріменко О. та Попов Р. [2], Шпатакова О., Іваненко Р. та Погребицький М. [3], Паньків Н., Чернишова А. [4], Пирога І., Пирога М. [6], Шевченко С., та Кукурудз О. [8]. звертають увагу на важливість ефективного відновлення критичної інфраструктури для стабільності та економічного розвитку країни після завершення війни. Іноземні дослідники Овенс М. (Owens M.) [5], Ліу М. (Liu M.), Джовіназі С. (Giovinazzi S.) [7], Порас-Гомез А.-М. (Porras-Gomez A.-M.) [9], Морі Ц. (Mori C.) [11] висвітлюють досвід інших країн у відновленні після воєнних конфліктів та надзвичайних ситуацій, що може бути корисним для України при розробці своїх власних стратегій.

Виклад основного матеріалу. Повномасштабне військове вторгнення Росії в Україну кардинально змінило реальність функціонування критичної інфраструктури. Щоденні ракетні удари, атаки дронів, артилерійські обстріли та диверсії спрямовані на знищення стратегічно важливих об'єктів, що призводить до значних економічних та соціальних втрат. Разом із фі-

зичними загрозами зростає рівень кібернетичних атак, спрямованих на порушення роботи енергосистем, банківського сектору, телекомунікацій та державного управління.

В умовах воєнного стану Україна змушена оперативно реагувати на загрози, адаптувати свою інфраструктуру до нових викликів, залучати міжнародну допомогу та шукати ефективні рішення для її захисту та відновлення.

Одним із головних напрямків ударів російських військ є енергетична інфраструктура. Протягом 2022–2023 років Україна пережила наймасштабніші атаки на енергосистему за всю історію незалежності. Внаслідок ударів були пошкоджені:

− Теплоелектростанції (ТЕС) та теплоелектроцентралі (ТЕЦ) – основні джерела теплопостачання та електроенергії для багатьох міст.

− Гідроелектростанції (ГЕС) – важливі об’єкти регулювання енергетичного балансу, які також забезпечують водопостачання.

− Атомні електростанції (АЕС) – ворог неодноразово обстрілював Запорізьку АЕС, створюючи загрозу ядерної катастрофи.

− Підстанції та лінії електропередач (ЛЕП) – їх пошкодження призводило до масштабних відключень електроенергії [5].

Наслідки таких атак були катастрофічними: мільйони українців залишалися без світла, тепла та води в зимовий період. Україна змушена була оперативно ремонтувати пошкоджені об’єкти та шукати альтернативні джерела енергії, зокрема генератори та імпорт електроенергії з Європи.

Згідно з дослідженнями, найбільшу частку загальних збитків становлять втрати у житловому секторі – приблизно $55,9 млрд., що включає у себе $1 млрд, який підрахований внаслідок затоплень та руйнувань житлових будинків під час підриву Каховської ГЕС. На другому місці за сумою збитків знаходиться сфера інфраструктури (транспортна, залізнична, дорожня, авіаційна та портова) – загалом $36,6 млрд. Втрати в активах бізнесу оцінюються на рівні $11,4 млрд. Варто зауважити, що пошкоджено або зруйновано принаймні 426 великих та середніх приватних підприємств та державних компаній. Проте кількість зруйнованих підприємств може бути великою, оскільки немає інформації щодо об'єктів на тимчасово окупованих територіях. Інфраструктурі української енергетики, за попередніми оцінками, завдано збитків на $8,8 млрд, з яких $638 млн становлять прямі збитки від підриву ГЕС [1].

Велика кількість енергетичних об'єктів, водопровідних систем, транспортних вузлів та іншої критичної інфраструктури стала мішенню нападів, що призвело до значних обмежень у доступі до електроенергії, водопостачання та транспортних маршрутів для населення, про що свідчать статистичні дані двох останніх років. За статистичними даними, більше половини об'єктів критичної інфраструктури в Україні зазнали руйнувань або серйозних пошкоджень [2].

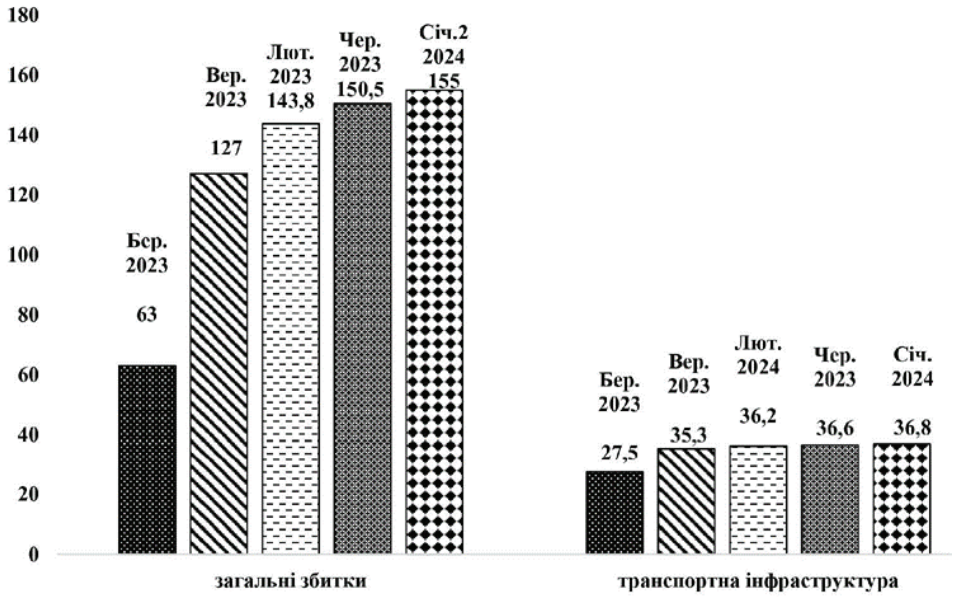

Рис. 1. Обсяги збитків критичної інфраструктури України протягом 2022–2023 років, млрд. $

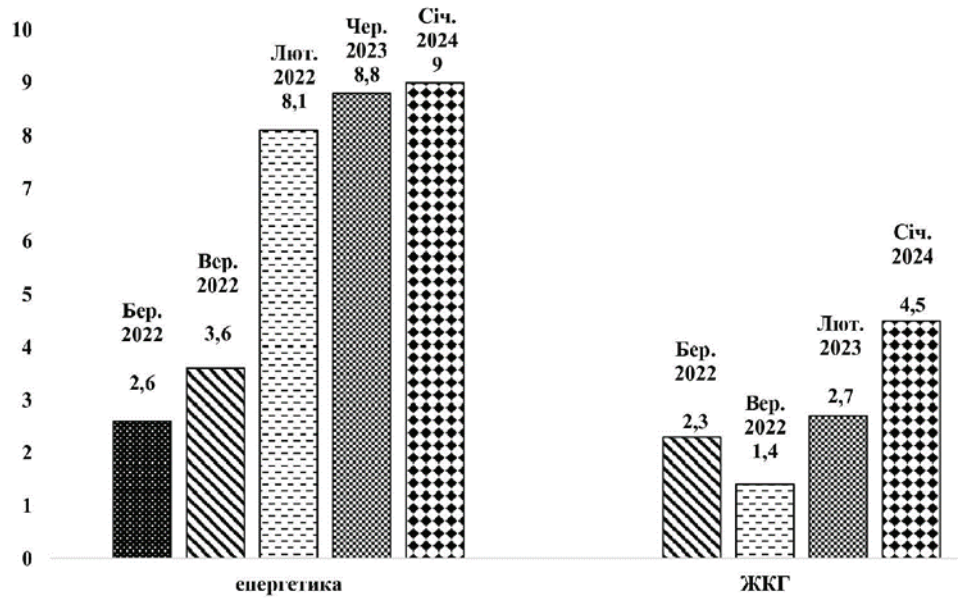

Рис. 2. Обсяги збитків енергетичної та ЖК інфраструктури України протягом 2022 – 2023 років, млрд. $

Залізничні вузли, мости, автомобільні дороги та порти є ключовими об'єктами для забезпечення логістики, перевезення вантажів та мобільності населення. Ворог систематично атакує транспортні шляхи, щоб:

− Перешкодити постачанню військової техніки та боєприпасів для українських Збройних сил.

− Ускладнити евакуацію мирного населення із зон активних бойових дій.

− Зруйнувати експортні можливості України, атакуючи порти та залізничні коридори [7].

Найбільшої шкоди зазнала інфраструктура південних і східних регіонів, де тривають активні бойові дії. Проте завдяки швидкому відновленню об'єктів, а також міжнародній підтримці Україна змогла зберегти функціональність залізничного транспорту та налагодити альтернативні шляхи експорту.

Руйнування насосних станцій, водогонів та очисних споруд створює критичні проблеми з водопостачанням у багатьох містах, зокрема в Харкові, Миколаєві та Запоріжжі. Ворог свідомо намагається створити гуманітарну кризу, позбавляючи людей доступу до чистої питної води.

Окупанти атакують великі промислові підприємства, що мають стратегічне значення для економіки та обороноздатності України. Найбільше страждають металургійні заводи, машинобудівні підприємства, нафтопереробні заводи та склади паливно-мастильних матеріалів. Це призводить до економічних втрат, зростання безробіття та проблем із постачанням паливних ресурсів [3].

Окрім фізичних атак, значну загрозу становлять кібернетичні атаки. Основні напрямки кібервійни проти України включають:

− Атаки на банківську систему – блокування роботи платіжних сервісів, злам баз даних, викрадення фінансової інформації.

− Дестабілізація енергосистеми – хакерські атаки на системи управління електромережами.

− Злам урядових сервісів та витік даних – спроби отримати секретну інформацію та вплинути на державне управління.

− Дезінформаційні кампанії – поширення фейкових новин для паніки та зниження довіри до влади [6].

Виявлення та аналіз ключових викликів та проблем, які стоять перед процесом відновлення об'єктів критичної інфраструктури в Україні після завершення війни, є критично важливим для розробки ефективних стратегій та механізмів відновлення. Розуміння цих проблем дозволить уникнути можливих перешкод та забезпечити ефективне використання ресурсів та зусиль для успішного відновлення інфраструктури.

Україна активно працює над захистом і відновленням критичної інфраструктури. Основні заходи включають:

1. Посилення протиповітряної оборони (ППО) – закупівля сучасних систем ППО для захисту енергетичних та промислових об'єктів.

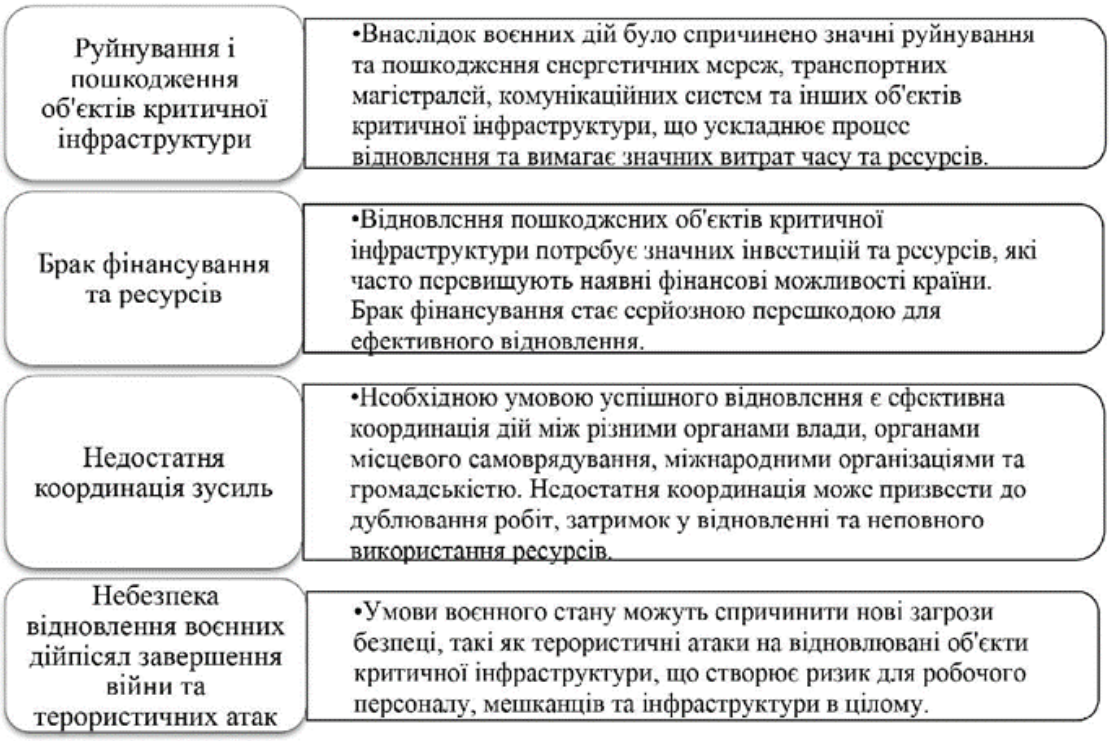

Рис. 3. Ключові виклики та проблеми, що виникають у процесі відновлення критичної інфраструктури

2. Розбудова резервних енергетичних потужностей – встановлення мобільних генераторів, сонячних електростанцій, вітрових електростанцій.

3. Захист кіберпростору – впровадження сучасних систем кібербезпеки, підготовка фахівців, співпраця з міжнародними партнерами.

4. Міжнародна допомога – залучення коштів та ресурсів для швидкого відновлення інфраструктури.

5. Децентралізація логістики – створення нових транспортних маршрутів для зменшення залежності від уразливих об’єктів [4].

Висновки і перспективи подальших розвідок у даному напрямі. Таким чином, війна в Україні висвітлила вразливість критичної інфраструктури, але водночас показала її здатність до швидкого відновлення. Захист енергетики, транспорту, зв’язку та інших ключових систем має стати пріоритетом державної політики. Майбутнє відновлення країни має базуватися на принципах безпеки, децентралізації, сталого розвитку та цифрової трансформації. Тільки завдяки комплексному підходу Україна зможе створити стійку та захищену інфраструктуру, здатну витримати будь-які виклики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. «Росія заплатить». Проєкт зі збору, оцінки й аналізу інформації про матеріальні втрати України від війни з Росією. Вебсайт. URL: https://kse.ua/ua/russia-willpay/

2. Охріменко О., Попов Р. Повоєнна відбудова України: потенціал та стратегія перетворень. Економіка та суспільство. 2022. 45. https://doi.org/10.32782/2524-0072/2022-45-7

3. Шпатакова О., Іваненко Р., Погребицький М. Перспективи відновлення критичної інфраструктури на деокупованих територіях України. Економіка та суспільство. 2022. 40. https://doi.org/10.32782/2524-0072/2022-40-5

4. Паньків Н., Чернишова А. Проблеми та перспективи відновлення України під час та після завершення російсько-української війни. *Вісник* Хмельницького національного університету. Економічні науки. 2023. № 1 (314). С. 67–79. https://doi.org/10.31891/2307-5740-2023-314-1-9

5. Owens M.D. Inter-state war, institutions and multinationals: insights from the Russian-Ukraine war. Multinational Business Review. 2023. Vol. 31 No. 4, pp. 496–517. https://doi.org/10.1108/MBR-05-2022-0067

6. Пирога І.С., Пирога М.І. Роль місцевого самоврядування у відбудові в умовах воєнного стану. *Науковий* вісник Ужгородського університету: серія: Право. 2023. Т. 1. Вип. 77. С. 117–123. https://doi.org/10.24144/2307-3322.2023.77.1.18

7. Liu M., Scheepbouwer E., Giovinazzi S. Critical success factors for post-disaster infrastructure recovery: Learning from the Canterbury (NZ) earthquake recovery. Disaster Prevention and Management. 2016. Vol. 25 No. 5, pp. 685–700. https://doi.org/10.1108/DPM-01-2016-0006

8. Шевченко С.О., Кукурудз О.М. Стратегії фінансування повоєнної відбудови: виклики та перспективи для України. Академічні візії. 2024. 28. https://doi.org/10.5281/zenodo.10678026

9. Porras-Gomez A.-M. The legal framework for the Syrian urban reconstruction. Journal of Property, Planning and Environmental Law. 2021. Vol. 13 No. 3, pp. 203–217. https://doi.org/10.1108/JPPEL-10-2020-0044

10. Організація економічного співробітництва та розвитку. Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками ОЕСР, Публікація ОЕСР, Париж. 2019. 110 с. https://doi.org/10.1787/02f0e5a0-e

Ковальов К.Є. СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ

У статті здійснено комплексний аналіз сучасних викликів і загроз для критичної інфраструктури України під час воєнного стану. В умовах повномасштабної збройної агресії значна частина об'єктів життєзабезпечення зазнала фізичних руйнувань через ракетні удари, артилерійські обстріли, диверсії та акти тероризму. Найбільших втрат зазнали енергетична, транспортна, комунікаційна, медична та промислова галузі, що спричинило серйозні перебої у функціонуванні економіки та забезпеченні базових потреб населення.

Окремий аспект дослідження присвячений кібернетичним загрозам, які суттєво посилилися в умовах війни. Російські хакерські угруповання здійснюють масовані атаки на урядові установи, фінансові організації, стратегічні підприємства та комунікаційні системи з метою дестабілізації державного управління, викрадення конфіденційних даних і створення хаосу в цифровому просторі. Особливу увагу приділено дезінформаційним кампаніям, які використовуються для підриву суспільної довіри, маніпулювання громадською думкою та психологічного тиску на населення.

У статті розглянуто заходи щодо посилення захисту критичної інфраструктури. Запропоновано ключові напрями вдосконалення системи безпеки, включаючи модернізацію систем протиповітряної оборони, створення резервних логістичних центрів, децентралізацію енергетичної інфраструктури, розвиток технологій кіберзахисту та впровадження механізмів моніторингу загроз. Висвітлено роль міжнародної співпраці у зміцненні обороноздатності критичних об'єктів, наданні матеріально-технічної допомоги та обміні досвідом у сфері цифрової безпеки.

Окреслено нормативно-правові аспекти захисту критичної інфраструктури України, необхідність реформування законодавчої бази та посилення координації між державним і приватним секторами. Запропоновано комплексний підхід до забезпечення безпеки, що включає державне управління, залучення бізнесу, міжнародне партнерство та використання сучасних технологій для оцінки ризиків і мінімізації потенційних загроз.

Стаття підкреслює важливість розробки довгострокових стратегій для забезпечення стійкості критичної інфраструктури в умовах війни та післявоєнного відновлення. Успішне подолання викликів вимагає комплексного підходу, інноваційних рішень та консолідації зусиль держави, громадянського суспільства і міжнародних партнерів.

Ключові слова: критична інфраструктура, воєнний стан, енергетична безпека, кіберзагрози, транспортна система, відновлення, цифрова безпека, національна безпека, нормативно-правове регулювання, міжнародна допомога, стійкість економіки, дезінформація, захист даних, протиповітряна оборона.

Kovalov K.Ye. MODERN CHALLENGES AND THREATS TO UKRAINE'S CRITICAL INFRASTRUCTURE DURING MARTIAL LAW

The article provides a comprehensive analysis of modern challenges and threats to Ukraine's critical infrastructure under martial law. Since the beginning of the full-scale armed aggression, critical infrastructure has suffered significant destruction due to missile strikes, artillery shelling, sabotage, and acts of terrorism. The energy system of the country has been hit the hardest, leading to widespread disruptions in electricity, heating, and the functioning of industrial enterprises. The transport infrastructure has also sustained severe damage, affecting the logistics of military and humanitarian supplies. As a result of attacks on telecommunication networks, there have been threats to communication and the operation of critical state bodies, weakening the ability to manage the state effectively during a crisis.

Special attention is given to cyber threats, which have significantly intensified during the war. Russian hacker groups are carrying out massive attacks on state institutions, financial organizations, strategic enterprises, and military information systems, aiming to destabilize the internal situation, steal secret data, and create digital chaos. In addition, an active information war is being waged: the spread of fake news, disinformation campaigns, and manipulations on social media are aimed at undermining trust in state institutions, inciting panic among the population, and discrediting Ukraine's international partners.

The article analyzes the main measures to strengthen the protection of critical infrastructure. A comprehensive approach to ensuring its security is proposed, including the modernization of the air defense system, the creation of reserve capacities for energy and transport infrastructure, and the implementation of modern technologies for detecting and neutralizing threats. Particular emphasis is placed on the importance of decentralizing key facilities, expanding the use of alternative energy sources, and implementing rapid-response mechanisms for emergencies.

A separate section of the article is dedicated to analyzing the legal and regulatory framework for the protection of critical infrastructure in Ukraine. The key issues of current legislation regulating the security of strategic facilities are identified, and directions for its improvement are suggested. Special attention is paid to the need for coordination between the public and private sectors, strengthening cooperation with international organizations and partners, and developing effective mechanisms for financing the restoration and modernization of infrastructure objects.

The issue of international support in the protection of Ukraine's critical infrastructure is also considered. The experience of European countries in ensuring the continuous functioning of strategic objects during crises and wars is analyzed. The potential for utilizing international grants, technological assistance, and expert consultations to enhance the security and resilience of Ukraine's key infrastructure sectors is outlined.

Overall, the article emphasizes the need for long-term strategies to strengthen the security of critical infrastructure during wartime and post-war recovery. Effectively addressing the threats requires an integrated approach, involving innovative technological solutions, expanded international cooperation, active participation of the public and private sectors, and the development of strategies for adapting to new challenges in the field of national security.

Key words*:* critical infrastructure, martial law, energy security, cyber threats, transport system, recovery, digital security, national security, legal regulation, international assistance, economic resilience, disinformation, data protection, air defense, strategic enterprises, public administration, cyber defense technologies, post-war recovery, telecommunication networks, information warfare, security coordination.