THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

Book of Conference Abstracts

The international scientific and practical conference

Berehove, 8–9 October 2025

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

International scientific and practical conference
Berehove, 8–9 October 2025

Book of Conference Abstracts

A BIZTONSÁG SZEREPE A HATÁRON ÁTNYÚLÓ ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2025. október 8–9.

Absztraktkötet

Міністерство освіти і науки України
Закарпатський угорський університет імені Ференца Ракоці II
Ужгородський національний університет

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

Університет Ракоці
Берегове
2025

УДК 004.056(063)(048.4)
Р 68

Збірник містить тези доповідей (українською, англійською та угорською мовами) міжнародної науково-практичної конференції «Роль безпеки в транскордонному та міжнародному співробітництві», яка відбулася 8–9 жовтня 2025 року в місті Берегове. Матеріали конференції висвітлюють широкий спектр проблем, пов'язаних із забезпеченням безпеки в умовах сучасних транскордонних та міжнародних викликів. Збірник тез доповідей охоплює питання політичних, соціальних, правових і технологічних аспектів безпеки, а також інтеграцію штучного інтелекту та цифрових технологій у систему захисту інформації. Організатори конференції: Закарпатський угорський університет імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Кафедра ЮНЕСКО «Неперервна професійна освіта XXI століття» НАПН України, Південноукраїнський національний педагогічний університет імені К. Д. Ушинського, Черкаський національний університет імені Богдана Хмельницького, Державний університет «Київський авіаційний інститут», Університет Григорія Сковороди в Переяславі, Міжнародний гуманітарний університет, Херсонський державний університет, Берегівський навчальний центр Матіасу Корвінусу Колегіуму, Пряшівський університет у Пряшеві, Жешувський університет, Ускюдарський університет, Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського університету імені Ференца Ракоці II
(протокол №12 від «17» грудня 2025 року)

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського університету імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом Університету Ракоці

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Оксана Мулеса та Ганна Мелеганич

Технічне редагування: *Адам Доровці, Олександр Добош та Анастасія Сенько*
Підготовка до видання у друкованій та електронній формі (PDF): *Анастасія Сенько*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша Університету Ракоці*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу Університету Ракоці)

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.

Проведення конференції та друк видання здійснено за підтримки уряду Угорщини.

Видавництво: Закарпатський угорський університет імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: egyetem@kme.org.ua; office@kme.org.ua)
Друк: ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua)

ISBN 978-617-8143-50-3 (м'яка обкладинка)
ISBN 978-617-8143-51-0 (PDF)

Ministry of Education and Science of Ukraine
Ferenc Rakoczi II Transcarpathian Hungarian University
Uzhhorod National University

THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

International scientific and practical conference
Berehove, 8–9 October 2025

Book of Conference Abstracts

University of Rakoczi
Berehove
2025

UDC 004.056(063)(048.4)
R 79

The book contains abstracts of presentations (in Ukrainian, English, and Hungarian) at the international scientific and practical conference “The Role of Security in Cross-Border and International Cooperation”, which took place on 8-9 October 2025 in Berehove. The conference materials highlight a wide range of issues related to ensuring security in the context of modern cross-border and international challenges. The book of conference abstracts covers political, social, legal, and technological aspects of security, as well as the integration of artificial intelligence and digital technologies into information protection systems. Organisers of the conference: Ferenc Rakoczi II Transcarpathian Hungarian University and Uzhhorod National University. Co-organisers: UNESCO Department "Continuous Professional Education of the 21st Century" of the National Academy of Sciences of Ukraine, K. D. Ushynsky South Ukrainian National Pedagogical University, Bohdan Khmelnytsky National University of Cherkasy, State University "Kyiv Aviation Institute", Hryhorii Skovoroda University in Pereiaslav, International Humanitarian University, Kherson State University, Berehove Training Center of Mathias Corvinus Collegium, University of Prešov, University of Rzeszów, Üsküdar University, Northern University Center of Baia Mare at Technical University of Cluj-Napoca.

Recommended for publication in printed and electronic form (PDF file format)
by the Academic Council of Ferenc Rakoczi II Transcarpathian Hungarian University
(record No.12 of December 17, 2025)

This volume of conference materials has been prepared by the Department of History and Social Sciences, the Department of Accounting and Auditing, the Department of Mathematics and Informatics at the Ferenc Rakoczi II Transcarpathian Hungarian University, and the Department of Systems Software, the Department of International Studies and Public Communications at the Uzhhorod National University, and the Division of Publishing at the University of Rakoczi.

Edited by:
Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D., Oksana Mulesa and Hanna Melehanych

Technical editing: *Adam Dorovtsi, Sándor Dobos and Anasztázia Szenykó*
Prepared for publication in printed and electronic form (PDF file format): *Anasztázia Szenykó*
Proof-reading: *the authors*
Cover design: *Vivien Tóth*
Universal Decimal Classification (UDC): *Apáczai Csere János Library of University of Rakoczi*

Responsible for publishing:
Sándor Dobos (head of the Division of Publishing of Ferenc Rakoczi II Transcarpathian Hungarian University)

Publications of research and teaching staff and students at the Uzhhorod National University were implemented within the framework of the state budget theme DB-921M “Information Security Protection in the Management of International Cooperation Projects on the Basis of Ensuring the National Security of Ukraine” with the support of the Ministry of Education and Science of Ukraine.

The conference and the publication of the conference abstracts sponsored by the government of Hungary.

Publishing: Ferenc Rakoczi II Transcarpathian Hungarian University (Address: Kossuth square 6, 90202 Berehove, Ukraine. E-mail: egyetem@kme.org.ua; office@kme.org.ua)
Printing: “RIK-U” LLC (Address: Carpathian Ukraine Street 36, 88006 Uzhhorod, Ukraine. E-mail: print@rik.com.ua)

ISBN 978-617-8143-50-3 (paperback)
ISBN 978-617-8143-51-0 (PDF)

Ukrajna Oktatási és Tudományos Minisztériuma
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
Ungvári Nemzeti Egyetem

A BIZTONSÁG SZEREPE A HATÁRON ÁTNYÚLÓ ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2025. október 8–9.

Absztraktkötet

Rákóczi Egyetem
Beregszász
2025

ETO 004.056(063)(048.4)
B 68

A tudományos kiadvány 2025. október 8–9-én, Beregszászban *A biztonság szerepe a határon átnyúló és nemzetközi együttműködésben* címmel megrendezett nemzetközi tudományos és szakmai konferencián elhangzott előadások absztraktjait tartalmazza ukrán, angol és magyar nyelven. Az előadások szerkesztett anyagai a biztonság biztosításával kapcsolatos széleskörű kérdéseket tárgyalják a mai határon átnyúló és nemzetközi kihívások összefüggésében. Az absztraktkötet a biztonság politikai, társadalmi, jogi és technológiai aspektusait, valamint a mesterséges intelligencia és a digitális technológiák integrációját is vizsgálja az információvédelem rendszerébe. A konferencia szervezői: a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem és az Ungvári Nemzeti Egyetem. Társszervezők: az Ukrán Nemzeti Pedagógiai Akadémia UNESCO „XXI. századi folyamatos szakképzés" Tanszéke, K.D. Usinszkij Dél-ukrajnai Nemzeti Pedagógiai Egyetem, Cserkaszi Bohdan Hmelnickij Nemzeti Egyetem, Kijevi Állami Repülőmérnöki Egyetem, Perejaszlavi Hrihorij Szkovoroda Egyetem, Nemzetközi Humántudományi Egyetem, Herszoni Állami Egyetem, a Mathias Corvinus Collegium Beregszászi Képzési Központja, Eperjesi Egyetem, Rzeszówi Egyetem, Üsküdari Egyetem és a Kolozsvári Műszaki Egyetem Nagybányai Északi Egyetemi Központja.

Nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra javasolta
a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem Tudományos Tanácsa
(2025. december 17., 12. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem Történelem- és Társadalomtudományi Tanszéke, Számvitel és Auditálás Tanszéke, Matematika és Informatika Tanszéke, Kiadói Részlege, valamint az Ungvári Nemzeti Egyetem Szoftverrendszerek Tanszéke, Nemzetközi Tanulmányok és Közszolgálati Kommunikáció Tanszéke.

Szerkesztette:
Csernicskó István, Maruszinec Marianna, Molnár D. Erzsébet,
Mulesza Okszána és Melehánics Anna

Műszaki szerkesztés: *Daróci Ádám, Dobos Sándor és Szenykó Anasztázia*
Előkészítés nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra: *Szenykó Anasztázia*
Korrektúra: *a szerzők*
Borítóterv: *Tóth Vivien*
ETO-besorolás: *a II. RF KMF Apáczai Csere János Könyvtára*

A kiadásért felel:
Dobos Sándor (a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem Kiadói Részlegének vezetője)

Az absztraktok tartalmáért és hitelességéért a szerzők viselik a felelősséget.
A szerzők álláspontja nem feltétlenül tükrözi a szerkesztők véleményét.

Az Ungvári Nemzeti Egyetem kutatói és oktatói munkatársainak és hallgatóinak publikációi Ukrajna Oktatási és Tudományos Minisztériumának támogatásával, a DB-921M „Az információbiztonság védelme a nemzetközi együttműködési projektek irányításában Ukrajna nemzetbiztonságának biztosítása alapján" című állami költségvetési projekt teljesítésének részeként készültek.

A konferenciát és a kiadvány megjelentetését
Magyarország Kormánya támogatta.

Kiadó: II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem (cím: 90 202, Beregszász, Kossuth tér 6. E-mail: egyetem@kme.org.ua; office@kme.org.ua)
Nyomdai munkálatok: „RIK-U" Kft. (cím: 88 006 Ungvár, Kárpáti Ukrajna u. 36. E-mail: print@rik.com.ua)

ISBN 978-617-8143-50-3 (puhatáblás)
ISBN 978-617-8143-51-0 (PDF)

ЗМІСТ / CONTENT / TARTALOM

Микола ПРОЦЕНКО
кандидат технічних наук, доцент
Державний університет інформаційно-комунікаційних технологій
m.procenko@duikt.edu.ua

МОДЕЛІ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ: СТАН І ПЕРСПЕКТИВИ

Безпека функціонування комп'ютерних мереж, напряму залежать від наявності засобів вчасного виявлення аномалій мережевому трафіку. Джерелами аномалій можуть бути різноманітні зловмисні дії: атаки типу "Відмова в обслуговуванні" (DoS/DDoS), несанкціонований доступ, сканування портів та зондування, спроби впровадження шкідливого коду, використання вразливостей захисту. Аномалії можуть створювати технічні збої чи нетипові закономірності в роботі обладнання. Традиційний захист брандмауери та системи IDS/IPS, сигнатурні системи виявлення атак мають суттєві обмеження, оскільки здебільшого орієнтовані на відомі патерни зловмисної активності.

У цьому контексті машинне навчання та методи штучного інтелекту відкривають нові можливості для аналізу мережевого трафіку, виявлення невідомих типів атак і, що важливо, створення адаптивних систем безпеки комп'ютерних мереж.

Статистичні методи аналізу трафіку ґрунтуються на статистичних показниках середніх значеннях, дисперсії, щільності розподілу. Аномалією вважається будь-яка подія, яка статистично значуще відхиляється від встановленого базового рівня. Методи прості в реалізації і не потребують значних обчислень, Деякі з них використовують часові ряди для прогнозування майбутніх рівнів трафіку та ідентифікації середньо- або довгострокових тенденцій. Недоліком методів слід вважати низьку стійкість до нестабільних умов роботи мережі, слабку здатність до виявлення складних атак із поступовою ескалацією.

Використання інтелектуальних алгоритмів значно розширило можливості визначення нетипових, а отже, потенційно небезпечних процесів в мережі. Інтелектуальні алгоритми стали основою сучасних систем виявлення вторгнень, заснованих на аномаліях (Anomaly-based Intrusion Detection Systems).

Машинне навчання (Machine Learning, ML) – це галузь штучного інтелекту, яка створює комп'ютерні моделі, здатні навчатися на зібраних даних, виявляти патерни та складати прогнозні рішення. Процес створення моделі проходить три етапи.

1. Вилучення ознак (Feature Engineering). Вручну вибираються ключові характеристики мережевого трафіку: обсяг трафіку за одиницю часу, кількість пакетів, середня тривалість сесії, кількість унікальних IP-адрес призначення.
2. Навчання моделі. Модель, наприклад, метод опорних векторів, навчається на великому обсязі нормального трафіку, щоб зрозуміти, що є «здоровою» поведінкою мережі.
3. Виявлення. Модель порівнює ознаки поточного трафіка з вивченою нормою. Якщо нові дані розміщуються далеко від визначених кластерів або виходять за встановлені статистичні межі, вони класифікуються як аномалія.

Клас методів класичного машинного навчання складають методи: «Опорних векторів» (Support Vector Machine, SVM) добре справляється зі структурованими даними, здатний відокремлювати нормальний трафік від аномального у багатовимірному просторі, використовує ядра для нелінійного розділення; «Дерева рішень, Випадковий ліс» (Decision Trees, Random Forest) забезпечує інтерпретацію моделей, здійснює аналіз важливості окремих ознак, що вказують на аномалію; «Найближчих сусідів» (k-NN) ефективний при роботі з відносно невеликими наборами даних або для виявлення локальних аномалій; «Кластеризації» (k-means, DBSCAN) дозволяє формувати групи «нормальних» та «аномальних» зразків без учителя, розглядаючи аномалії як точки, що не належать до жодного кластера (DBSCAN, ізоляція) або далекі від центру нормального кластера (k-means).

Позитивними сторонами методів є відносна простота реалізації, наявність апробованих бібліотек та алгоритмів. Водночас методи потребують ретельний підбір патернів, на їхні можливості негативно впливає зростання інтенсивності та нестабільна динамічність трафіку.

Глибинне навчання (Deep Learning, DL) це підмножина ML. Для обробки даних DL використовує глибинні нейронні мережі (Deep Neural Networks, DNN) – мережі з кількома прихованими (проміжними) шарами. На сьогоднішній день, в сфері виявлення аномалій трафіку, методи DL є найперспективнішими. До класу мереж DNN відносяться: «Рекурентні нейронні мережі» (RNN, LSTM, GRU) ефективні для аналізу часових послідовностей пакетів у трафіку; «Автокодери» (Autoencoders) здійснюють відновлення нормальних патернів з реального трафіку; великі відхилення між параметрами реального і відновленого трафіка вказують на аномалії; «Нейронні мережі на графах» (Graph Neural Networks, GNN) враховують топологію мережі та зв'язки між вузлами; «Генеративно-змагальні мережі» (Generative Adversarial Network, GAN) створюють нові зразки трафіку чим підвищують точність виявлення рідкісних атак.

Позитивні сторони DNN: висока точність, здатність обробляти дані великих обсягів та виявляти складні нелінійних залежності. Негативні: значні обчислювальні витрати, потреба у великих обсягах даних для навчання, складність інтерпретації результатів.

Практика показала, що моделі глибинного навчання мають вищу точність у порівнянні з класичними алгоритмами. Водночас дослідники стикаються з проблемою узагальненості: алгоритми, добре навчені на певних вибірках, часто втрачають ефективність у випадку застосуванні до реального трафіку, де характер атак і поведінка користувачів постійно змінюються. Серед позитивних аспектів моделей DL слід відзначити підвищену здатність виявляти невідомі раніше аномалії, гнучкість і масштабованість, можливість використання у хмарних сервісах і на розподілених обчислювальних платформах. Водночас моделі DL мають високу потребу в обчислювальних ресурсах, допускають значну кількості хибних спрацювань, характеризуються складністю налаштування для реальних мережевих середовищ.

Підводячи підсумок, можна сказати, що моделі машинного навчання є потужним інструментом виявлення аномалій мережевого трафіку, на даний час вони демонструють високу ефективність у дослідницьких експериментах. Водночас на шляху до їх широкого практичного впровадження існує низка проблем: брак актуальних даних, складність адаптації до мінливих умов і недостатня інтерпретаційність. Подальший розвиток галузі пов'язаний із гібридними та адаптивними підходами, інтеграцією пояснюваного AI (Explainable AI, XAI) та розробкою методів, здатних працювати в реальному часі у високонавантажених розгалужених мережах.

Фахівці в галузі ML зазначають, що моделям машинного навчання притаманна здатність до вдосконалення і розвитку. В цьому аспекті визначені наступні перспективні напрямки:

1. Інтеграція гібридних моделей. Поєднання статистичних методів, класичного ML та глибинного навчання для досягнення балансу між точністю та швидкістю.
2. Адаптивне навчання. Використання онлайн- та інкрементального навчання для динамічного підлаштування під зміни в трафіку.
3. Федеративне навчання. Об'єднання локальних моделей із різних організацій без обміну самими даними, що дозволить враховувати ширший спектр сценаріїв атак.
4. Пояснюваний штучний інтелект (XAI). Розробка методів, які не лише виявляють аномалії, а й пояснюють причини їх класифікації.
5. Оптимізація під IoT та 5G. Легковагові моделі для пристроїв із обмеженими ресурсами та мереж нового покоління.
6. Використання генеративних моделей. GAN можуть допомогти створювати реалістичні сценарії атак для тестування систем.

Таким чином, майбутнє моделей ML полягає у поєднанні інтелектуальних алгоритмів і практичних механізмів їх використання, що дасть змогу ефективніше протидіяти новим кіберзагрозам та підвищити стійкість комп'ютерних мереж.

УДК 004.056(063)(048.4)
Р 68

Роль безпеки в транскордонному та міжнародному співробітництві. Наукове видання (Збірник тез доповідей) Закарпатського угорського університету імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Оксана Мулеса та Ганна Мелеганич. Берегове: Університет Ракоці, 2025. – 384 с. (українською, англійською та угорською мовами)

ISBN 978-617-8143-50-3 (м'яка обкладинка)
ISBN 978-617-8143-51-0 (PDF)

Збірник містить тези доповідей (українською, англійською та угорською мовами) міжнародної науково-практичної конференції «Роль безпеки в транскордонному та міжнародному співробітництві», яка відбулася 8–9 жовтня 2025 року в місті Берегове. Матеріали конференції висвітлюють широкий спектр проблем, пов'язаних із забезпеченням безпеки в умовах сучасних транскордонних та міжнародних викликів. Збірник тез доповідей охоплює питання політичних, соціальних, правових і технологічних аспектів безпеки, а також інтеграцію штучного інтелекту та цифрових технологій у систему захисту інформації. Організатори конференції: Закарпатський угорський університет імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Кафедра ЮНЕСКО «Неперервна професійна освіта XXI століття» НАПН України, Південноукраїнський національний педагогічний університет імені К. Д. Ушинського, Черкаський національний університет імені Богдана Хмельницького, Державний університет «Київський авіаційний інститут», Університет Григорія Сковороди в Переяславі, Міжнародний гуманітарний університет, Херсонський державний університет, Берегівський навчальний центр Матіасу Корвінусу Колегіуму, Пряшівський університет у Пряшеві, Жешувський університет, Ускюдарський університет, Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Наукове видання

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

2025 р.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського університету імені Ференца Ракоці II
(протокол №12 від «17» грудня 2025 року)

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського університету імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом Університету Ракоці

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д,
Оксана Мулеса та Ганна Мелеганич

Технічне редагування: *Адам Доровці, Олександр Добош та Анастасія Сенько*
Підготовка до видання у друкованій та електронній формі (PDF): *Анастасія Сенько*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша Університету Ракоці*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу Університету Ракоці)

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.

Проведення конференції та друк видання здійснено за підтримки уряду Угорщини.

Видавництво: Закарпатський угорський університет імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: egyetem@kme.org.ua; office@kme.org.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції Серія ДК 8485 від 23 жовтня 2025 року*.
Друк: ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції Серія ДК 5040 від 21 січня 2016 року*

Шрифт «Times New Roman».
Папір офсетний, щільністю 80 г/м². Друк цифровий. Ум. друк. арк. 31,2.
Формат 70x100/16.

ISBN 978-617-8143-50-3