

**Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Науково-дослідна лабораторія
з проблемних питань кримінального аналізу**

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

**Матеріали
Міжнародної науково-практичної конференції
22 листопада 2019 року**

Одеса
ОДУВС
2019

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)
К 38

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № 5 від 12 грудня 2019 року)

**Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції**

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. 108 с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 22 листопада 2019 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)

ISBN 678-717-7020

© ОДУВС, 2019

у період масового використання всесвітньої мережі Інтернет, набуває актуальності адміністративно-правовий аспект кібернетичної безпеки у державних органах України.

Сприйняття Україною поняття кібербезпеки поки досить загальне, проте ведеться робота по цьому напрямку. Для комплексної боротьби з кібератаками потрібні спільні зусилля держави, міжнародної спільноти та громадян. На разі проблемою кібербезпеки країни займаються різні відомства: Міністерство внутрішніх справ, Державна служба спеціального зв'язку і захисту інформації, Національне агентство з питань запобігання корупції, Національний банк, Служба безпеки України та інші, кожне з них веде статистику відповідних показників та вживає заходи щодо безпеки, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Цілісний напрямок та політика у питанні кібернетичної безпеки країни поки відсутні, як і універсальні індикатори заходів, що могли б охарактеризувати рівень кібербезпеки.

Національним агентством з питань запобігання корупції (далі — НАЗК) 10 червня 2016 року прийнято рішення (zareestrovano в Міністерстві юстиції України 15 липня 2016 року за № 958/29088) про початок роботи системи електронного декларування з 1 вересня 2016 року [1]. На сьогоднішній день громадянам України, котрі займають державну посаду, потрібно декларувати статки. Кожного року громадяни України декларують свої статки в електронному форматі, але після періоду декларування, на суди України надходять безліч позовів за порушення вимог фінансового контролю, як від самих громадян та і від контролюючих органів. На що громадяни України пояснюють, що не мають ніякого умислу на вчинення адміністративного правопорушення, так само як і не мають ніякого корупційного інтересу при цьому, мети приховати зміни своїх статків не переслідують, оскільки громадянами, котрі реєструють свої електронні декларації, здійснювались неодноразові спроби подати повідомлення про зміни в майновому стані на Інтернет-сторінці НАЗК, з метою його вчасного заповнення і подання, однак не можуть цього зробити через перебої в роботі сервісу, перебоями у внутрішній мережі Інтернет в зв'язку з кібератаками, відсутністю електропостачання в суді, що також підтверджується списками справ призначених до розгляду та актами Тиврівського районного суду Вінницької області за №19 від 26.06.2017 року та №20 від 27.06.2017 року [2]. Це одна з наведених прикладів судової справи через несправність та кібератаки на сервери сайту НАЗК, у той період коли сервери перебувають найбільш завантаженими, а саме у період звітності громадян. На сьогодні НАЗК має дві основні проблеми: це перевантаженість сайту у період звітності та кібератаки, наприклад таке шкідливе ПЗ (Malware) – створення та розповсюдження вірусів і шкідливого програмного забезпечення. Таку кібератаку зазнали багато держорганів України, Malware є хакерська атака вірусом під назвою Petya (також відомий як Petya.A, Petya.D, Trojan.Ransom.Petya, PetrWrap, NotPetya, ExPetr, GoldenEye), котрий був запущений у березні 2016 року. Ця програма котра шифрує файли на жорсткому диску комп'ютера жертви, а також перезаписує і шифрує MBR - дані, необхідні для завантаження операційної системи.

Для того щоб сьогодні НАЗК змогла протидіяти таким кібератакам, на наш погляд потрібно:

- 1) підвищити рівень кваліфікації фахівців в органах захисту національної безпеки країни;
- 2) використовувати світовий досвід країн, котрі мають позитивні результати у боротьбі з кіберзлочинністю;
- 3) постійно оновлювати ліцензоване програмне забезпечення;
- 4) оновлювати та удосконалювати сервери збереження даних.

Окремі питання використання електронних доказів при розслідуванні кіберзлочинів

Сіренко О.В.

доцент кафедри кримінального процесу та
криміналістики

Університет державної фіскальної служби України
к. ю. н.

Кіберзлочин – це кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за яке передбачено кримінальну відповідальність [6, с.48].

«Стрибок» кількості всіх кіберзлочинів відбувся у 2017 році, значною мірою він пов'язаний з вірусом Petya. Відтоді, кількість інформаційних злочинів не зменшується. В 2017 році було зафіксовано 1795 справ, в 2018 – 1023, за останні півроку – 1005. На даний момент в судовому реєстрі є 1500 справ [4].

Зростання кількості кіберзлочинів обумовлюється удосконаленням технічних і програмних засобів, доступних для зловмисників, і посилюється існуванням нелегального ринку з продажу засобів для здійснення кіберзлочинів.

Як зазначають науковці, «кіберзлочини, на відміну від традиційних, мають низку характерних особливостей, серед яких слід зазначити такі: - місце вчинення кіберзлочину, на відміну від традиційних, може знаходитись в різних юрисдикціях – правопорушник активізує кібератаку, наприклад, з Інтернет-кафе однієї країни, бот-мережа знаходиться в іншій, а атакована інформаційна система – у третій; - переважна кількість доказів кіберзлочинів існують в електронній формі (так звані “електронні” або “цифрові” докази). Вони, на відміну від традиційних, можуть швидко знищуватися чи модифікуватися. Для їх отримання, зберігання та аналізу необхідне спеціалізоване обладнання; - внаслідок специфічної природи кіберпростору постраждалим не завжди обізнаний про вчинення кіберзлочину тощо» [3, с.119].

Як зазначають фахівці, «першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину: визначення типу електронно-обчислювальної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування; встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ (Unix, Linux, Netware, Windows), а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звужити коло можливих підозрюваних; визначення апаратного та програмного забезпечення, яке піддалося впливу під час неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину» [2, с.179].

Під час проведення розслідування кіберзлочинів особливу увагу приділяють збиранню доказів. Відповідно до положень кримінального процесуального кодексу, «сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених Кримінальним процесуальним кодексом» [5].

Доказами в кримінальному провадженні є «фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів» [5].

Відповідно до ч. 1 ст. 99, «документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [5].

До документів, за умови наявності в них відомостей, передбачених частиною першою, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні).

Електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [9].

Електронний документ є досить вразливим, оскільки він може бути легко змінений, знищений тощо. Саме ця його риса, на думку науковців, зумовлює «необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема,

на рівні з традиційними правилами поведінки із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації» [8, с. 82].

Слід погодитись з позицією науковців, які серед не врегульованих та проблемних аспектів використання електронних доказів у кримінальному судочинстві виокремлюють: відсутність чіткого процесуального порядку їх отримання відповідно до кримінального процесуального кодексу України; відсутність підстав визнання електронних доказів недопустимими; відсутність сформованої методики дослідження таких доказів; складності у слідчих під час виявлення та фіксації електронних доказів через недостатність спеціальних знань у слідчих, що зумовлює необхідність залучення спеціалістів для проведення процесуальних дій; відсутність однотипної термінології та урегульованості на законодавчому рівні [1, с.248-249].

Поняття електронних доказів та електронних документів потребує закріплення на законодавчому рівні, а також, з огляду на проблеми, які виникають в процесі виявлення і фіксації доказів через можливість зміни а то і знищення «віртуальних слідів» доказів, нагальним є питання формування методики дослідження електронних доказів, порядок їх збирання та фіксації.

Література:

1. Алексеева-Процюк Д.О. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування *Науковий вісник публічного та приватного права*. 2018. Випуск 2. С.247 – 253.
2. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали Міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ, 2013. С. 179–182
3. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності *Інформація і право*. 2019. № 1(28). С. 118 - 128
4. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років - Opendatabot. URL: <https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zroslo-vdvichi-za-ostanni-p-yat-rokiv-opendatabot>
5. Кримінальний процесуальний кодекс України: Науково-практичний коментар / Відп. ред.: С. В. Ківалов, С. М. Міщенко, В. Ю. Захарченко. Х.: Одиссей, 2013. 1104 с.
6. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх розслідування *Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ.конф., м. Одеса. ОДУВС, 2017. С.48-49*
7. Фурман В. Кіберзлочинність. Проблеми доказування Аналітичне видання “Юрист&Закон”. Випуск №45. URL: <https://artius.ua/novini/statti/kiberzlochinist-problemi-dokazuvannya.html>
8. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень *Держава та регіони*. №4 (58). 2017. С.80 – 85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf
9. Цивільний процесуальний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/1618-15>.

Кібертероризм: поняття та шляхи протидії

Форос Г. В.

доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
к.ю.н., доцент

Ільченко Д.І., Узюм П.А.

курсанти 301 взводу

Одеського державного університету внутрішніх справ

Найбільш вагомою проблемою сучасного світу, що виникає разом із стрімким розвитком інформаційних технологій та глобальної мережі Інтернет, є поява нових видів злочинів, зокрема кібертероризму. Під кібертероризмом розуміється суспільно небезпечна діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на ІТС з використанням високих технологій [1, с. 57].

СЕКЦІЯ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ В УКРАЇНІ

Гончаров М.В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства.....	4
Даніч М.А. Проблеми кваліфікації та криміналізації фішингу.....	5
Коротун О.М. Кібербезпека та інтелектуальна власність: питання правового забезпечення.....	7
Щирська В.С., Слободянюк А.В. Кримінальна відповідальність за злочини вчиненні у сфері кіберпростору.....	9
Нашинець-Наумова А.Ю. Кібершпідіаж - загроза сучасному інформаційному суспільству.....	11
Панасюк О.Т. Кібербезпека як (трудо)правоутворюючий чинник.....	13
Максимчук І.Р., Божок С.Г. Національне законодавство із забезпечення кібербезпеки в Україні.....	15
Мамедова Е.А., Мирошніченко В.О. Правові засади забезпечення кібербезпеки держоргану «Національне агентство з питань запобігання корупції».....	17
Сіренко О.В. Окремі питання використання електронних доказів при розслідуванні кіберзлочинів.....	18
Форос Г.В., Ільченко Д.І., Узюм П.А. Кібертероризм: поняття та шляхи протидії.....	20
Чижов Д. А. Кіберзлочинність: поняття, види, загрози та ризики.....	22

СЕКЦІЯ 2
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ В УКРАЇНІ

Кушнір І.П. Актуальні засади захисту інформації, що обробляється в автоматизованих системах державної прикордонної служби України.....	25
Рибальченко Л.В., Гребенюк А.М. Стандарти управління інформаційною безпекою.....	26
Постол О.І. Технологічне насильство як сучасна форма домашнього насильства.....	27
Бурцева І.В., Божок С.Г. Кіберзлочинність в Україні: види, наслідки та способи боротьби.....	29

Семенов А.О., Божок С.Г.

Система забезпечення кібербезпеки в Україні: сутність та призначення.....31

Титаренко І.В.

Забезпечення кібербезпеки в управлінні організацією праці на підприємстві.....33

Жогов В.С.

Проблеми адміністративно-правового регулювання хмарних технологій в аспекті розповсюдження об'єктів авторських і суміжних прав, виражених у цифровій формі.....34

Пелюх Р.Р., Маковій В.П.

Захист прав та інтересів особи внаслідок розміщення недостовірної інформації щодо неї в мережі Інтернет.....37

Ребрик О.О., Маковій В.П.,

Здійснення авторських прав в Інтернеті.....39

СЕКЦІЯ 3 ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Грохольський В.Л.

Аналіз та прогнозування криміногенної ситуації підрозділами кримінальної поліції України.....42

Vladislav Cojuhari

Perspectives and issues of using the biometricsystems in crimes combatting.....44

Бабенко К.А.

Ефективність систем інформаційної безпеки у навчальному та науковому державному закладі.....46

Гавриш О.С.

Вразливості Android-смартфонів.....48

Курило В. І.

До питання протидії комп'ютерній злочинності в кібернетичному просторі.....49

Дідик В.О., Коркін О.Ю., Симоненков В.М., Коновець В.І.

Підвищення ситуаційної поінформованості наземних роботизованих комплексів на підтримку мережецентричної концепції ведення бойових дій.....51

Доценко О.С.

Використання інформаційних технологій організованими злочинними формуваннями.....52

Фоменко А., Вишня В.

Комп'ютерні засоби для боротьби з крадіжками вантажів на залізничному транспорті України.....54

Ковтун В. О., Світличний В. А.

Способи та методи попередження та протидії легалізації доходів, одержаних у сфері кіберзлочинності 57

Кудінов В.А.

Рекомендації щодо основних шляхів створення належного рівня захищеності Єдиної інформаційної системи МВС України.....59

Махницький О.В.

Методи оцінки безпеки комп'ютерних систем.....61

Мельнікова О.О., Дзіковська Н.Р.

Використання інформаційних технологій в розслідуванні злочинів.....62

Павлова Н.В.

Роль спеціаліста у технічному забезпеченні проведення слідчих (розшукових) дій.....64

Первій В.Ю.

Особливості діяльності правоохоронних органів України в рамках сучасних інформаційних технологій.....65

Петрівський В.Я., Шевченко В.Л., Шевченко А.В.

Інформаційні системи протидії функціональній нестабільності програмного забезпечення.....67

Поліневич О.В., Супрун-Ковальчук Т.М.

Сучасна система запобігання корупції в Україні та її вдосконалення.....68

Русило М.О., Мирошніченко В.О.

Використання сучасних технологій відеоаналітики в органах Національної поліції.....70

Шевченко О.І., Форос Г.В.

SRS Femida – сучасна система технічної фіксації судового процесу.....71

Щирська В.С., Зварич Р.А.

Використання інформаційних технологій під час розслідування злочинів.....73

Форос Г.В., Кірей Д.В.

Інформаційно-аналітичний документ як результат інформаційно-аналітичної діяльності.....74

Форноляк В.М.

Особливості співробітництва правоохоронних органів країн ЄС у сфері протидії кібертероризму.....76

Цільмак О.М.

Метод фактологічного аналізу як один із методів доказування.....78

СЕКЦІЯ 4

ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Моїсеєнко К.Д., Полуніна Л.В.

Актуальні аспекти підготовки кадрів з попередження кіберзлочинності в Україні.....80

Косаревська О.В.

Актуальні питання впровадження інформаційно-комунікативних технологій у навчально-виховний процес ЗВО з особливими умовами навчання у сфері протидії кіберзлочинності.....82

Радова М.Р., Лісніченко Д.В.

Місце аналітиків в правоохоронній системі України.....83

Форос Г.В.

Психологічні особливості осіб, які вчиняють злочини у сфері високих технологій.....85

СЕКЦІЯ 5

**ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ
У БОРОТБІ ЗІ ЗЛОЧИННІСТЮ**

Мельнікова О.О., Шаран А.А.

Деякі проблеми взаємодії слідчого з оперативними та інформаційно-аналітичними підрозділами Національної поліції України.....88

Орлов В.В.

Звуколокація безпілотних літальних апаратів в задачах попередження терористичних погроз.....90

Котко А.О., Кузьменко Ю.В.

Кібербезпека – важливий напрям діяльності органів державної влади щодо захисту суспільства.....91

Ігнатушко Ю.І.

Інформаційне суспільство в Україні.....93

Матвєєвський О.В.

Актуальні проблеми проведення судових експертиз під час розслідування воєнних злочинів.....95

Мельнікова О.О., Ісмаїлов К.Ю.

Інформаційно-аналітичне забезпечення та особливості здійснення пошуку осіб, які становлять оперативний інтерес у злочинах, пов'язаних з торгівлею людьми.....96

Мудрецька Г.В.

Проблемні питання захисту персональних даних при використанні інформаційних систем та технологій в боротьбі зі злочинністю.....98

Пекарський С.П.

Прикладні аспекти фахової підготовки працівників кіберполіції 100

Теслюк І.О.

Криміналістичний моніторинг як метод боротьби з кіберзлочинністю.....101

**Міжнародна науково-практична конференція
Кібербезпека в Україні: правові та організаційні питання
15 листопада 2020 року
м. Одеса, Україна**

ЗАПРОШЕННЯ

Інформуємо Вас, що **15 листопада 2020 року** в м. Одеса відбудеться Міжнародна науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання».

Для участі в конференції запрошуються вчені, співробітники науково-дослідних установ, аспіранти, курсанти, студенти.

Робочі мови конференції: українська, англійська, російська.

ПОДАННЯ ДОКУМЕНТІВ:

Для участі в конференції представити наступні документи:

1. Заявку у відповідності з формою;
2. Тези доповіді на одній із робочих мов, оформлені у відповідності із запропонованим зразком;

ПУБЛІКАЦІЯ ПРАЦЬ КОНФЕРЕНЦІЇ

Тези доповідей, отримані Організаційним комітетом та прийняті до друку, будуть видані до початку конференції у збірнику праць конференції та вислані безкоштовно на електронні адреса учасників конференції.

АДРЕСА ОРГКОМІТЕТУ:

Кафедра кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Адреса: вул. Успенська, 1, м. Одеса, 65000, Україна
Сайт: <http://oduvs.sem-dev.co.ua/kafedra-kiberbezpeki-ta-informatsijnogo-zabezpechennya/>
E-mail: 0997060070@ukr.net
facebook: <https://www.facebook.com/kiberoduvs>

Контактні особи:

Ісмайлов Карен Юрійович +38 (099) 70-600-70;
+38 (097) 70-600-90;
0997060070@ukr.net

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

**Матеріали
Міжнародної науково-практичної конференції**

22 листопада 2019 року

Підписано до друку 12.12.2019. Формат 60х90/8. Папір офсетний.

Гарн. «Times New Roman» Друк цифровий. Ум. друк арк. 26,1.

Наклад 500 прим.

Видавництво ОДУВС

м. Одеса, вул. Успенська, 1

Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.

тел. 0487024884; 0949547884 email – ndrvv1@gmail.com