

**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. 110 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

- спеціальне навчання працівників, щодо користування комп'ютерною технікою, програмним забезпеченням та електронними носіями;
- проходження спеціальних психологічних тренінгів щодо виявлення неправомірних дій зовнішніх користувачів та інших осіб по використанню комерційних даних;
- здійснення постійного контролю в поточній роботі, в здійснених вчинках та плануванні майбутніх заходів;
- виявлення можливих загроз та їх запобігання в межах комплексу необхідних дій;
- конфіденційність управлінської інформації для працівників, які нею володіють;
- відповідальність кожного працівника за збереження операцій на комп'ютерних носіях;
- обмін інформацією між працівниками щодо безпеки інформації на підприємстві.

Слід відзначити, що управління кібербезпекою входить до загальної системи управління економічною безпекою підприємства, і залежно від розмірів та потужності підприємства.

З метою попередження неправомірного втручання у комп'ютерну інформацію та попередження злочинів із використанням даних пропонуємо створити належну систему захисту цієї інформації, з використанням таких принципів:

- якісне використання та підтримка програмного забезпечення;
- захист конфіденційної інформації;
- персональна відповідальність;
- секретність;
- комплексність заходів;
- контроль доступу до облікових даних;
- розробка правил та процедур на підприємстві по системі безпеки;

Слід відзначити, що до основних напрямків по удосконаленню організаційного забезпечення системи кібербезпеки на підприємстві та якісного управління організацією праці можна запропонувати розробку документу щодо політики правил захисту інформації та інструкції по поведінці працівників апарату управління, а також створення спецслужби та спец комісії щодо регулювання кіберзахисту на підприємстві. Розробка та затвердження нових документів надасть змогу логічній послідовності дій та забезпеченню максимального захисту інформації. Для ширшого розуміння та правомірного використання матеріальних та трудових ресурсів пропонуємо ввести розділ до Наказу про облікову політику підприємства з розкриттям усіх необхідних правил та дій у веденні бухгалтерського обліку, резерву витрат, пов'язаних з кібербезпекою та внутрішнім контролем на підприємстві.

За допомогою вище перелічених заходів щодо безпеки в управлінні організацією праці на підприємстві, можна досягнути високих результатів роботи та системності захисту управлінської інформації.

Література:

1. Про внесення змін до Закону України «Про основи національної безпеки України»: проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. URL www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998
2. Про Національну програму інформатизації : закон України від 4.02.1998 р. №74/98-ВР URL: <http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>
3. Дубов Д.В., Ожеван М.А.. Кібербезпека : світові тенденції та виклики для України. К. : НІСД, 2011. 30 с.

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

Жогов В.С.

ад'юнкт кафедри кібербезпеки
та інформаційного забезпечення

Одеського державного університету внутрішніх справ

В останні кілька років хмарні технології увійшли в десятку найбільш популярних стратегічних комп'ютерних технологій, зайнявши вирішальну позицію серед ресурсних інтересів комерційних підприємств і представників бізнесу в силу високої потенціальної можливості знижувати вартість витрат на комп'ютерне та технологічне забезпечення. Представникам же малого бізнесу вони дозволяють вийти на більш високі рівні ринку без необхідності витрачатися на підтримку ефективності

роботи комп'ютерної техніки, а також витратити істотні матеріальні ресурси на закупівлю програмного забезпечення або технічних носіїв.

Міжнародна інформаційна корпорація (International Data Corporation (IDC)) в 2012 р спрогнозувала, що протягом найближчого десятиліття більше 80% нових комерційних додатків для бізнесу буде створюватися винятково на базі хмарних технологій [1]. Європейська комісія також передбачає, що розвиток хмарних технологій буде додавати до ВВП Євросоюзу до 250 млрд євро на рік, а до 2020 р сукупний вплив на економіку за період з 2015 р до 2020 р оцінюється в 600 млрд євро [2].

В одному з досліджень, що стосуються такого способу передачі і обробки інформації йдеться, що основна мета сучасних комп'ютерних технологій полягає у знищенні бар'єрів між інформаційними послугами [3]. Це виражається саме в тому, що сучасні технології не залежать більше від географічного положення провайдера послуг і ефективність ринку таких послуг прямо похідна від швидкості доступу, наданого користувачу, незалежно від місця його знаходження. Такі зміни ускладнили законодавче регулювання захисту об'єктів авторського права, виражених у цифровій формі і, в той же час, вивели їх на міжнародний рівень не тільки в правовому сенсі, а й у фактичному.

Варто підкреслити, що в правових системах різних країн існують схожі норми регулювання відносин в даній сфері. Так, в законодавстві США застосовується доктрина сумлінного використання творів (англ. Fair use) [4] та Закон США «Про захист авторських прав у цифрову епоху» (Digital Millennium Copyright Act) [5]. В країнах ЄС діє Директива ЄС N 2000/31 / ЄС «Про деякі правові аспекти інформаційних послуг на внутрішньому ринку, зокрема, про електронну комерцію» [6].

У той час як законодавство зарубіжних країн зробило крок далеко вперед у питанні регулювання відносин, що формуються при використанні хмарних технологій, постійно доповнює і вдосконалює його з урахуванням швидко мінливих технологічних і соціальних умов надання хмарного сервісу, Україна поки не визначилася у виборі загальної стратегії регулювання таких відносин.

Сьогодні робляться численні спроби створення експертних рад, комісій і робочих груп для створення нормативного правового акта, що регулює відносини, що виникають при використанні хмарних технологій. І до тих пір, поки відсутнє спеціальне регулювання відносин, що виникають при використанні хмарних технологій, до таких відносин доведеться застосовувати існуюче законодавство і тільки в тій частині, яка хоч скільки-небудь може бути застосовна.

Звісно ж, що правове регулювання відносин, що виникають при використанні хмарних технологій, до сих пір є дискусійною темою в багатьох аспектах, в тому числі в питаннях охорони авторського права і суміжних прав на результати інтелектуальної діяльності.

На думку А. Бережного проблеми відсутності чіткого нормативного регулювання відносин, пов'язаних з хмарними технологіями, а також можливі ризики втрати даних або доступності таких послуг не дозволяють повністю покластись на сумлінність постачальника хмарних послуг, що спричиняє необхідність розвитку нормативно-правової бази та механізмів контролю за її дотриманням [7].

При використанні хмарних технологій важливо дотримуватись законодавчих вимог до обробки персональних даних та іншої інформації, що може бути незаконно використана іншими. Крім того, максимально чітко повинен проводитися облік результатів від використання таких послуг, з обов'язковим розмежуванням з постачальником послуг прав на одержувані результати.

Тема «хмар» є дуже актуальною і породжує безліч дискусій та запитань. Недарма, дві доповіді на секції «VII Міжнародного форуму «Інтелектуальна власність - XXI століття», присвячені правовій охороні комп'ютерних програм, так або інакше торкалися проблеми хмарних технологій, що виникають у зв'язку з їх використанням. Зокрема, було відзначено, великий вплив на новий підхід до розуміння авторського права зробило впровадження хмарних технологій [8].

На сьогоднішній день в практиці не розроблений механізм визначення, чи правомірно відбувається поширення того чи іншого твору за допомогою мережі Інтернет. Це питання постійно хвилює розуми вчених і авторів. Звісно, визначити правомірність використання твору, викладеного в Facebook, дуже складно, відповідно подальше правомірне використання такого твору з урахуванням норм законодавства ставиться під питання.

Складніша ситуація з неправомірним використанням авторських творів, створених та/або які розповсюджуються при використанні хмарних технологій. Користувач хмарного сервісу вступає у відносини з приводу твору, авторські права на яке належать третій особі, при цьому твір виражено в цифровій формі та створено або розміщено з використанням хмарного сервісу таким чином, що інші користувачі можуть отримати доступ до такого об'єкта в будь-який час і з будь-якого місця, керуючись лише власним бажанням.

Таким чином, виходить, що основні труднощі виникають тоді, коли користувачі мають можливість завантажувати або вивантажувати об'єкти інтелектуальної діяльності та здійснювати їх копіювання та розповсюдження.

З огляду на актуальність тематики, в офісі Microsoft Ukraine було проведено семінар на тему «Використання хмарних технологій у бізнесі», на якому представники компанії розповіли про можливості їхнього програмного забезпечення, а також виступили доповідачі від юридичної фірми «Saenko Kharenko», які стверджують про необхідність обов'язкового законодавчого регулювання цієї сфери, оскільки норми чинного законодавства не адаптовані до регулювання правовідносин із застосуванням сучасних технологій [9]. На нашу думку, до проблем хмарних технологій можна також віднести й відсутність методологічної бази щодо взаємодії контролюючих органів з правоохоронними органами в даній сфері.

Можна сказати, що розвиток «хмарних технологій», розширення їх можливостей та велику кількість сфер використання вимагає від законодавця розробки нормативно-правової бази у сфері хмарних технологій, оскільки розповсюдження конкретно хмарної послуги може виходити за географічні межі країни, в якій вона була створена, оскільки більшість великих хмарних провайдерів є резидентами США, Китаю або Євросоюзу. Тому у деяких сферах діяльності для оцінки можливості використання «хмарних» сервісів слід враховувати спеціальне регулювання, яке передбачає застосування особливих засобів і технологій захисту інформації, наприклад, обмеження зберігання інформації за межами України.

Одночасно з цим розвиваються й місцеві оператори хмарних технологій, які користуються популярністю в нашій державі, тому й їх діяльність також потребує національного нормативного регулювання.

Таким чином, незважаючи на те, що законодавство в області інтелектуальної власності постійно вдосконалюється, використання стрімко розвиваються технологій може сприяти визнанню чинного законодавства в сфері інтелектуальної власності застарілим, що може зумовити підміну законодавчого регулювання звичаями ділового обороту, договірної практики, щоб хоч якось регулювати ці процеси. У зв'язку з цим ми вважаємо необхідним внести поправки в чинне законодавство в частині забезпечення охорони об'єктів авторського права виражених в цифровій формі при використанні хмарних послуг.

Література:

1. Gens, F. IDC Predictions 2012: Competing for 2020 [Електронний ресурс]. – Режим доступу: <http://www.virtustream.com/sites/default/files/IDCTOP10Predictions 2012.pdf>.
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.09.2012. COM (2012) 529 final [Електронний ресурс]. – Режим доступу: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>.
3. Vaquero L. M., Rodero-Merino L., Caceres J., Lindner M. A Break in the Clouds: Towards a Cloud Definition. SIGCOMM Computing Community Review, 2009, vol. 39 (1), p. 50–55.
4. CopyrightAct, UnitedStatesCode/Title17 // Режим доступу: <http://www.copyright.gov/title17/>.
5. DigitalMillenniumCopyrightAct, DMCA // Режим доступу: <https://www.aclu.org/text-digital-millennium-copyright-act-dmca>.
6. Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 «On certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)» // Режим доступу: http://www.wipo.int/wipolex/ru/text.jsp?file_id=181678.
7. Бережной А. Облачные вычисления: Новое или хорошо забытое старое? // Режим доступу: <http://samag.ru/archive/article/1214>
8. VII МЕЖДУНАРОДНЫЙ ФОРУМ «ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ – XXI ВЕК»: Журнал «Экономические стратегии» («ЭС») Режим доступу: <http://www.inesnet.ru/2014/04/vii-mezhdunarodnyj-forum-intellektualnaya-sobstvennost-xxi-vek/>
9. «Хмарні» технології в бізнесреаліях України: Всеукраїнське щотижневє професійне юридичне видання «Юридична Газета» Режим доступу <http://jur-gazeta.com/publications/actual/hmarni-tehnologiyi-v-biznesrealiyah-ukrayini.html>

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.

Кібершпівонаж - 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 БОРОТБІ 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 кіберзлочинності57

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., Мирошниченко 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., Лісниченко 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 БОРОТЬБІ 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 кіберполіції100

Теслюк І.О.

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

Курбатова І.С.

Аналіз стану злочинності як складова інформаційного забезпечення правоохоронної діяльності.....103

Козаченко О.І.

Міжнародний досвід, як елемент вдосконалення правового регулювання інституту викривачів та інституту негласного інформування правоохоронних органів.....105

Коломісць А.М.

Наркополітика європейських країн, як ключовий вектор для України.....109

Гордієнко С.Г.

Технологія протидії конкурентній розвідці.....110

**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