

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ**

**МАТЕРІАЛИ
Всеукраїнської
науково-практичної конференції**

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ



**21 жовтня 2016 року
м. Одеса**

*Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»*

Міністерство внутрішніх справ України

Одеський державний університет внутрішніх справ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали

Всеукраїнської науково-практичної конференції

21 жовтня 2016 року

Одеса
ОДУВС
2016

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 № 4 від 03 листопада 2016 року)

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

**Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ.
К38 конф., м. Одеса, 21 жовтня 2016 р. – Одеса : ОДУВС, 2016. – 232 с.
ISBN 678-717-7020**

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на всеукраїнську науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 21 жовтня 2016 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 та технологій в боротьбі з кіберзлочинністю 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

Нормативно-правові засади використання високотехнологічних і програмних інструментів у боротьбі з кіберзлочинністю

Лефтеров Л.В.

старший інспектор Департаменту Кіберполіції НП України,
ад'юнкт кафедри кримінального права та кримінології ОДУВС

Бабенко А.М.

доктор юридичних наук, доцент
професор кафедри кримінального права і кримінології
Одеського державного університету внутрішніх справ

Темпи інноваційного розвитку при сьогоденному змаганні технологій дуже високі. Кожен день розробляється більше 100 тисяч нових зразків шкідливого програмного забезпечення. За деякі шкідливі програмні модулі сплачуються суми, які перевищують мільйон доларів. За оцінкою Центра стратегічних і міжнародних досліджень (Center for Strategic and International Studies) збиток від кіберзлочинності для світової економіки становить понад 445 мільярдів доларів на рік[3].

Згідно з висновками звіту організації, які хочуть проявляти пильність, повинні бути готові виявити будь-яку атаку. Швидка мобілізація включає в себе раннє визначення напряду дії загрози і причини атаки. Також швидкі дії, кваліфіційні навички та вміння використовувати у своїй діяльності високотехнологічні і програмні інструменти повинні бути присутніми у працівника підрозділів боротьби з кіберзлочинністю.

Розділ II Конституції України з метою захисту прав і свобод громадян, забезпечує таємницю листування, недоторканність особистих даних, заборону збирання особистих даних [1, ст. 21-29]. Однак вказані права – виключають можливість швидкого реагування за тяжкими кіберзлочинами та особливо тяжкими злочинами загального характеру в яких використовуються електронно обчислювальні мережі.

Основними принципами якісного та результативного реагування у зазначених вище випадках, є виявлення «гарячих слідів», що були залишені зловмисником. Основним фактором отримання електронної інформації є порядок повноцінного аналізу і упорядковування відомостей наданих потерпілою стороною. З інцидентами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, відповідальність за які передбачена Розділом 16 Кримінального кодексу України, одним з основних доказових чинників є результати запису інформації про події з об'єктами (в рамках комп'ютерної мережі, або з автоматизованою системою). Цей процес також називається аудитом, дані про який вкладаються системою у файл с записами про події у хронологічному порядку (файл реєстрації, протокол, журнал або лог-файл).

Лог-файли можуть містити вичерпну інформацію про:

- загальні дані про дії з ядром системи (контроль доступу програм в мережу);
- завантаження системи (зберігає основні системні події, журнал операційної системи);
- дані про звернення до сервера, інформацію щодо помилок веб-сервера (логи веб-сервера);
- запити до баз даних, помилки сервера (логи сервера баз даних);
- спроби входу в панель, поновлення ліцензії та панелі, статистику використання ресурсів сервера (логи хостингової панелі);
- дані щодо всіх відправлених і доставлених повідомлень, помилки поштового сервера (логи поштового сервера);
- дані щодо виявлення шкідливого програмного забезпечення у системі (журнал антивірусної програми).

З нормативно-правової точки зору, аналізування наданих протоколів, не є порушенням процесуального законодавства, а навпаки на етапі первинної перевірки факту, надає змогу визначити безпосередню кваліфікацію кримінального правопорушення [4, ст. 16].

Використання програмних та високотехнологічних інструментів для аналізування лог-файлів є невід'ємною частиною якісного розкриття кіберзлочинів. Насамперед, слід зазначити, що технічні характеристики файлів журналу мають формат тексту або таблиць, що дозволяє у своїй діяльності використовувати комп'ютерні текстові редактори та пакети офісних додатків, з функцією сортування і пошуку даних.

Отриману в ході аналізу електрону інформацію слід використовувати для подальшого збору доказів в рамках кримінального провадження. Частіше за все при пошуку осіб використовуються інформація про IP-адреси.

IP-адреса це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах [5, ст. 113]. Аналізування IP-адрес або доменних імен Веб-сайтів здійснюється за допомогою вільних сервісів які працюють за Інтернет протоколами «WHOIS». Сервіси WHOIS використовується для запитів до бази даних, щодо визначення власника доменної зони, отримання відомостей про IP-адресу, або автономного системного номера в Інтернеті. Згідно вимог ICANN (Internet Corporation for Assigned Names and Numbers - міжнародна некомерційна організація, щодо регулювання питань, пов'язаних з доменними іменами, IP-адресами і іншими аспектами функціонування Інтернету) та «Угоди про акредитацію реєстраторів» від червня 2013 року, в рамках реєстрації доменних імен та IP-адрес в WHOIS, реєстратор повинен представити, або розмістити в базі даних реєстру наступні елементи даних:

- Ім'я реєстратора;
- найменування оператора або провайдера (щодо належності IP-адрес);
- контактні дані реєстратора або оператора (провайдера);
- первісна дата створення реєстраційної записи;
- дата закінчення терміну реєстрації;
- найменування та поштову адресу власника зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з технічних питань для зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з адміністративних питань для зареєстрованого імені [6].

Слід зазначити, що до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини [2, ст. 21]. Аналіз та збирання цифрової інформації у вигляді IP-адрес не є конфіденційними даними про фізичну особу. Також інформація не є конфіденційною, якщо особа самостійно надала згоду на її опублікування та обробку. У цьому випадку якісним програмними інструментами виступають самостійно сформовані бази даних загально доступних соціальних мереж.

Подібних масиви даних, також можуть нести в собі помилкову або неправдиву інформацію, тому важливо використання у своїй діяльності все більших сервісів та програмних інструментів що можуть допомогти у боротьбі з кіберзлочинністю. Високотехнологічні і програмні інструменти можуть застосовуватись на всіх етапах кримінального процесу та використовуватись у якості доказової бази. Неодмінним фактором долучення отриманих відомостей у якості доказів до кримінального провадження є їх допустимість. Саме в цьому випадку підготовка усіх даних повинна проводитись згідно чинного законодавства.

Література:

1. Конституція України / Відомості Верховної Ради України від 23.07.1996 — 1996 р.;
2. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N 48);
3. Report: Cybercrime and espionage costs \$445 billion annually [Електронний ресурс] // Washingtonpost. – 2014. – Режим доступу до ресурсу: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html;
4. Юрасов А.В. Основы электронной коммерции / А. В. Юрасов., 2008. – 480 с. – (Телеком);
5. Комп'ютерні мережі / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.;
6. Соглашение об аккредитации регистраторов [Електронний ресурс] // icann. – 2013. – Режим доступу до ресурсу: <https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru>

ЗМІСТ

ПЛЕНАРНЕ ЗАСІДАННЯ

Катеринчук І.П. Правоохоронні органи в боротьбі з кіберзлочинністю.....	4
Албул С.В. Протидія інформаційним загрозам в умовах антитерористичної операції.....	7
Грохольський В.Л. Адміністративно-правові заходи боротьби з кіберзлочинністю в Україні	9
Карчевский Н.В. Киберпреступление или преступление в сфере использования информационных технологий?	10
Грищук Р.В. Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни.....	16
Пядишев В.Г. Місце кібертероризму в структурі кіберзлочинності та напрями боротьби з ним.....	17
Лефтеров Л.В., Бабенко А.М. Нормативно-правові засади використання високотехнологічних і програмних інструментів у боротьбі з кіберзлочинністю	19
Ісмаїлов К.Ю., Мусаєва С.С. Особливості забезпечення кібернетичної безпеки України в сучасних умовах розвитку кіберпростору.....	21

СЕКЦІЯ 1

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Головка О.М., Савінова Н.А. Вплив на людську свідомість в медіапросторі як інформаційна загроза сучасності.....	24
Маковій В.П., Бабенко Т.С. Співвідношення публічного та приватного інтересу у межах протидії кіберзлочинності.....	26
Делія Ю.В. Захист інформаційної діяльності органів публічного адміністрування в Україні.....	28
Бібік І.С., Бабенко А.М. Вплив Інтернету як фактор вчинення неповнолітніми злочинів проти життя та здоров'я особи у регіонах України.....	30
Сверба Ю.І., Березовська Н.Л. Деякі питання кримінально-правової характеристики DDOS-атаки.....	33
Мукоїда Р.В., Шелехов А.О. Законодавство України у сфері боротьби з кіберзлочинністю.....	35

Березовська Н.Л. Кібербезпека як об'єкт кримінально-правової охорони.....	37
Шуміло О.О., Голіна В.В. Щодо актуальності імплементації міжнародних стандартів кібербезпеки до національного законодавства України.....	38
Дорохіна Ю.А. До проблеми розуміння кіберзлочинів проти власності.....	40
Задніченко С.І. Комп'ютерна програма як одна зі складових неправомірної вигоди.....	42
Іващенко Ю.К., Черняк Н.П. Кібербезпека в Україні: сучасний стан.....	43
Калініна І.В. Правова природа та доказове значення висновку експерта у кримінальних провадженнях про кіберзлочини.....	45
Кришечевич О.В. Кримінальна відповідальність за комп'ютерне шахрайство – один з елементів кіберзлочинності	47
Солдатенко О.А., Гурагов А.П. Психологічний аспект слідчих та співробітників оперативних підрозділів під час досудового розслідування кримінальних правопорушень.....	49
Солдатенко О.А., Легкий М.І. Принцип поваги до людської гідності під час кримінального процесу.....	50
Солдатенко О.А., Любова Н.О. Експерт як важливий учасник кримінального процесу.....	51
Форос Г.В., Козуменко Є.І. Спеціальний суб'єкт злочину в сфері інформаційної безпеки.....	53
Форос Г.В., Никитюк В.С. Щодо особливостей правового забезпечення інформаційної безпеки.....	55
Теслюк І.О., Цільмак О.М. Криміналістичне прогнозування як стратегічний метод при проведенні обшуку.....	56
Андрусенко С.В., Горбенюк Т.А. Правове регулювання забезпечення безпеки осіб залучених до проведення негласних слідчих (розшукових) дій.....	58
Бараненко Р.В., Вікторов Д.І. Дослідження факторів, що впливають на вчинення кіберзлочинів.....	60
Делія Ю.В., Власенко А.В. Протидія торгівлі людьми в мережі Інтернет.....	63
Ісмайлов К.Ю., Никитюк В.О. Передові юридичні доктрини в інформаційному праві в період незалежності України.....	64

Мукоїда Р.В., Шелехов А.О.

Використання правоохоронними органами сучасних інформаційно-аналітичних технологій у протидії тіньовій економіці в Україні.....	66
---	----

Біба А.В., Пекарський С.П.

Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту і розповсюдженню порнографічних предметів.....	68
--	----

Пекарський С.П., Кушнарєва К.О.

Компетенція кіберполіції з протидії ввезенню, виготовленню, збуту або розповсюдженню творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію.....	70
--	----

Хлевицький В.Б.

Окремі проблеми правового забезпечення кібернетичної безпеки в Україні в умовах розвитку інформаційного суспільства.....	72
--	----

Шелехов А.О., Корнієнко М.В.

Використання європейського досвіду в організації роботи поліції України.....	74
--	----

Небеська М.С.

Сучасні проблеми кіберзлочинності: міжнародний аспект.....	77
--	----

Небеська М.С., Свиріпа І.В.

Актуальні питання нормативно-правового забезпечення аналітично-інформаційної системи Національної поліції України.....	79
--	----

СЕКЦІЯ 2

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Нікітенко О.І., Журавель І.В.

Адміністративно-правове регулювання у сфері забезпечення кібербезпеки в Україні.....	82
--	----

Козюра В.Д., Хорошко В.О.

Створення системи кібернетичної безпеки в Україні: деякі актуальні питання.....	83
---	----

Манжай О.В.

Особливості безпечної роботи з інформацією в МВС та Національній поліції України.....	85
---	----

Делія Ю.В., Кіянчук В.М.

Кібербезпека інтелектуальної власності у відкритій мережі інтернет.....	86
---	----

Манжай І.А.

Аналіз активності у деструктивних мережних співтовариствах для прогнозування сплесків протиправної діяльності.....	88
--	----

Нашинець-Наумова А.Ю.

Парадигмальна трансформація концепції інформаційної безпеки.....	89
--	----

Добровольська О.О., Даніч М.А.

Деякі психологічні особливості осіб, які вчиняють злочини у сфері високих технологій.....	91
---	----

Політова А.С. Термінологічна невизначеність у сфері кібербезпеки.....	92
Гончаров М.В. До питання кібернетичної безпеки в Україні.....	94
Припутень Д.С., Кожушина О.В. Сутність та зміст громадського порядку і його адміністративно-правової охорони.....	96
Скачкова Т.Ю. Початкові дії спеціаліста під час огляду місця події за фактом порушення працездатності комп'ютерної системи.....	97
Форос Г.В., Баркар Р.І. Кібертероризм як різновид тероризму.....	99
Форос Г.В., Кондрашева К.С. Інформаційне суспільство та кібербезпека.....	101
Форос Г.В. Щодо розмежування понять «кібербезпека» та «інформаційна безпека».....	102
Косаревська О.В., Новіцький О.І. Протидія кіберзлочинності як складова інформаційної безпеки держави.....	104
Косаревська О.В., Шутило С.В. Кіберзлочини у фінансово-банківській сфері: скілінг та способи його викорінення.....	106
Бараненко Р.В., Гітрук О.О. Кібербезпека як один із факторів забезпечення національної безпеки держави.....	108
Бухонський С.О. Щодо сучасного стану інформаційно-аналітичного забезпечення початкового етапу досудового розслідування та перспективи його розви.....	110
Романов О.Д., Касюк О.О. Кібератаки і кібертероризм: поняття та особливості реалізації атак у кіберпросторі.....	113
Ігнатушко Ю.І. Проблеми розслідування злочинів щодо порушення авторського права на комп'ютерні програми.....	115
Ком'яга А.В. Актуальні питання адміністративно-правового забезпечення кібербезпеки в Україні	117
Бааджи Н.А. Проблеми визначення поняття адміністративного розсуду.....	118
Любчик В.Б., Слободянюк О.О. Кіберзлочинність як злочин транснаціонального характеру	120
Медведенко С.В., Колодніцький Р.Р. Роль та місце зворотного зв'язку в процесі здійснення управлінської діяльності.....	122
Мукоїда Р.В., Аносенков А.А. Створення інформаційного середовища взаємодії та роботи у сфері запобігання та протидії легалізації (відмиванню) доходів.....	125

Розовик І.В., Шевчук О.Ю.

Кіберзлочинність в Україні: перспективи протидії.....127

Саакян М.Б.

Правове регулювання поширення інформації в мережі Інтернет.....128

Нерубащенко І.Ю., Янковий М.О.

Особа злочинця як елемент криміналістичної характеристики злочинів у сфері мобільних телекомунікацій.....131

СЕКЦІЯ 3 ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Кузьменко Б.В.

Використання інформаційних технологій і систем на підприємствах енергетики України.....133

Казакова Н.Ф., Фразе-Фразенко О.О., Щербина Ю.В.

Сучасні проблеми оцінки захищеності інформаційно-телекомунікаційних систем.....134

Осадчий Є.О., Горбунов О.А.

Методи та засоби таймерного захисту інформації.....136

Хахановський В.Г., Єгоров Д.А.

Основні правові аспекти використання інформаційних технологій у боротьбі з кіберзлочинністю в Україні: проблематика та шляхи вирішення.....138

Стрельбицький М.А., Ваврічен О.А.

Приховані канали витоку інформації в інформаційно-телекомунікаційних системах Державної прикордонної служби України та шляхи їх ліквідації.....140

Хахановський В.Г., Дабіжа Д.В.

Використання інформаційних систем для візуального аналізу даних в боротьбі з кіберзлочинністю.....142

Larysa Kupriianova, Daryna Kupriianova

Act of the forensic medicine: main features of the storage an access to theevident database. The main ways of protecting electronic versions of the medical documents in Ukraine and Poland.....145

Коваленко А.В., Смирнов А.А., Коваленко А.С.

Разработка метода управления рисками разработки программного обеспечения.....146

Волинець Д.О., Чесановський І.І.

Оцінка технологій радіо доступу з метою реалізації в телекомунікаційній мережі.....148

Кудінов В.А.

Методика оцінки рівня кібербезпеки в Україні.....151

Кушнір І.П.

Правове забезпечення захисту інформації пов'язаної із охороною державного кордону.....152

Мелешко Є.В.

Дослідження методів динамічного аналізу віртуальних соціальних мереж з точки зору інформаційної безпеки.....154

Миколенко О.М.

Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.....155

Мирошниченко А.И., Лещенко О.И.

Перспективы использования пористого кремния в качестве датчиков систем с контролем доступа157

Шестак Я.В., Оксуюк А.Г.

Модель построения киберзащищенного информационного пространства ЦОД: Математический аспект.....159

Одарченко Р.С., Гнатюк С.О.

Принципи формування вимог до систем безпеки мереж 5G.....160

Зерко А.Л., Оксуюк О.Г.

Дослідження методів класифікації захищених операційних систем за варіантами їх використання.....162

Коновець В.І., Симоненков В.М., Черниш І.А.

Особливості використання криптозахищених автоматичних ідентифікаційних судових станцій.....163

Пеньков С.В.

Дослід США щодо застосування оперативної техніки у протидії злочинності.....164

Косаревська О.В.

Інформаційно-пошукові системи в діяльності поліцейських.....166

Орлик О.В.

Інформаційні технології забезпечення безпеки електронного бізнесу.....167

Балтовский А.А., Сифоров А.И.

Подстройки коэффициентов модели управления как методика процедуры адаптации.....169

Форос Г.В., Підващевська Л.В.

Визначення проявів корупційних правопорушень в інформаційній сфері.....171

Форос Г.В., Щур К.В.

Діяльність України у сфері боротьби з кіберзлочинністю.....173

Форос Г.В., Бадюк М.О.

Деякі аспекти щодо проблем запобігання та протидії кіберзлочинності.....174

Деркач В.А., Деркач І.І.

Інформаційні технології в поліцейській діяльності.....176

Храпкіна В.В., Храпкін О.М.

Сутність та роль кібербезпеки в сучасному суспільстві.....178

Черняк Н.П.

Проблеми боротьби з кіберзлочинністю у сучасних умовах становлення України.....179

Ісмайлов К.Ю., Гладковський Е.О.

Криптографічні методи захисту інформації: види та вимоги до них.....181

Білоусов А.С.

Слідчий огляд в справах про комп'ютерні злочини.....183

Власенко І.М.

Аналіз окремих вразливостей технології ss7 в мережах мобільного зв'язку.....185

Мельнікова О.О., Мишко В.В.

Інформаційно-аналітичне забезпечення оперативного пошуку ознак злочинів,
пов'язаних з торгівлею людьми.....186

Рвачов О.М., Беляєва Є.Г.

DDoS-атаки: їх вплив на безпеку інформації, способи захисту.....189

СЕКЦІЯ 4 ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Рижков Е.В., Тітов О.О.

Пошукінформації яка становить оперативний інтерес, в мережі Інтернет.....191

Пекарський С.П.

Деякі питання системи фахової підготовки працівників кіберполіції
у вищих навчальних закладах МВС України.....194

Санаков Д.Б.

Засоби протидії неправомірному контенту підрозділами кіберполіції України:
міжнародний досвід.....196

Соловйов О. Ю., Казакова Н.Ф.

Особливості підготовки фахівців по боротьбі з кіберзлочинністю.....198

Деля Ю.В., Барган С.С.

Боротьба зі шкідливим програмним забезпеченням в сучасному кіберсередовищі.....199

Доценко В.В.

Використання тренінгових технологій у підготовці персоналу
для боротьби з кіберзлочинністю.....201

Калюга К.В.

Питання встановлення закономірностей, що лежать в основі утворення криміналістично
значущої інформації.....202

Малихін В.А.

Підготовка майбутніх інженерів-педагогів до забезпечення безпеки
інформаційних систем в освітньому середовищі.....204

Мілорадова Н.Е., Кислинська Д.М.

Формування системи ціннісних орієнтацій майбутніх правоохоронців.....206

Мілорадова Н.Е.

Тренінг розвитку професійних настановлень у підготовці фахівців для боротьби з
кіберзлочинністю208

Муляр Т.М.

Особливості підготовки фахівців у сфері публічного управління.....209

Онищенко Ю.М., Черновол В.С.

Особливості підготовки фахівців для підрозділів боротьби з кіберзлочинністю.....210

Світличний В.А.

Аналітична обробка інформації в діяльності поліції Харкова.....212

Пасько О.М.

Підготовка персоналу для боротьби з кіберзлочинністю на вузівському рівні.....213

Савченко В.С.

Професіограма слідчого в контексті набуття ним психологічних навичок
розслідування злочинів у сфері використання комп'ютерних технологій.....215

Кравченко В.О., Черняк Н.П.

Особливості підготовки персоналу для боротьби з кіберзлочинністю в Україні.....216

Корнієнко М.В., Підващеська Л.В.

Особливості управління в територіальних органах національної поліції.....218

Поляков Є.В., Гонтарук Е.Л.

Кібертероризм як загроза національній безпеці України.....221

Наукове видання

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

**Матеріали
Всеукраїнської науково-практичної конференції**

21 жовтня 2016 року

Підписано до друку 03.11.2016. 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