МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Кафедра кримінального процесу

OSINT

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для підготовки до практичних занять та самостійної роботи
здобувачів першого (бакалаврського) рівня вищої освіти
в галузі знань 12 «Інформаційні технології»

Одеса
2025

УДК 343.1:303.6 (477) (073) + 343.1:303.7 (477) (073)

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(*протокол № 4 від «10» лютого 2025 р.*)

Укладачі:

Аркуша Л.І., доктор юридичних наук, професор, завідувач кафедри криміналістики, детективної та оперативно-розшукової діяльності, Голова Комітету з питань юридичної освіти та науки НААУ

ORCID iD: *https://orcid.org/0000-0002-0422-6416*

Дикий О.В., кандидат юридичних наук, доцент, декан Факультету кібербезпеки та інформаційної діяльності, доцент кафедри кримінального процесу

ORCID iD: *https://orcid.org/0000-0001-9659-9350*

Мандриченко Ж.В., кандидат юридичних наук, доцент, доцент кафедри кримінального процесу

ORCID iD: https://orcid.org/0000-0002-9114-3044

Стоянов М.М., кандидат юридичних наук, доцент, доцент кафедри кримінального процесу

ORCID iD: https://orcid.org/0000-0003-4948-3288

Сидорчук В.В., доктор філософії в галузі права, старший викладач кафедри кримінального процесу

ORCID iD: https://orcid.org/*0000-0001-8457-1633*

Рецензенти:

Подобний О.О. – д.ю.н., професор, завідувач кафедри кримінального права, процесу та криміналістики Міжнародного гуманітарного університету;

Цехан Д.М. – д.ю.н, професор, професор кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія».

OSINT : метод. реком. для підготовки до практ. занять та самост. роботи здобув. першого (бакалаврського) рівня вищ.осв. галузі знань 12 «Інформаційні технології» [Електронне видання] / уклад.: Аркуша Л.І., Дикий О.В., Мандриченко Ж.В., Стоянов М.М., Сидорчук В.В.; Нац. ун-т «Одеська юрид. академія». Одеса, 2025, 55 с. URL: https://hdl.handle.net/11300/29233

Методичні рекомендації призначені для підготовки до практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти в галузі знань 12 «Інформаційні технології», з метою закріплення лекційного матеріалу і підготовки до практичних і самостійних занять з дисципліни «OSINT».

УДК 343.1:303.6 (477) (073) + 343.1:303.7 (477) (073)

© Л.І. Аркуша, О.В. Дикий, Ж.В. Мандриченко,
М.М. Стоянов, В.В. Сидорчук, 2025

ЗМІСТ

ВСТУП

Навчальна дисципліна «OSINT» призначена для здобувачів, які навчаються за освітньою програмою підготовки бакалаврів з галузі знань 12 «Інформаційні технології» в Національному університеті «Одеська юридична академія».

Навчальна дисципліна «OSINT» присвячена знайомству здобувачів з видом діяльності, направленим на збір, обробку, аналіз інформації з відкритих джерел, та подальшій презентації висновків, які були зроблені на основі аналізу. В ході її вивчення буде досліджено поняття OSINT, суміжних категорій, сфери застосування OSINT, проведено аналіз найактуальніших OSINT розслідувань, класифіковано джерела інформації для OSINT розслідування, розглянуто відкриті бази даних як джерело для аналітики, визначено етапи відповідної діяльності, розглянуто наявні інструменти для OSINT аналітики, досліджено правові аспекти отримання і використання інформації під час OSINT розслідувань, надано поняття відкритих джерел їх видів та класифікації, а також зазначено можливі ризики в ході здійснення OSINT розслідування.

Предмет навчального курсу складає діяльність направлена на отримання, обробку, аналіз та презентацію інформації з відкритих джерел.

Метою відповідного курсу є надання уявлення про існуючий вид діяльності, її етапи, інструментарій, правові аспекти отримання і використання інформації та ризики, пов’язані з відповідним видом діяльності.

Основними **завданнями** курсу є:

- надання визначення OSINT та порівняння його з суміжними поняттями;
- дослідження найактуальніших OSINT розслідувань;
- визначення кола інструментарію OSINT діяльності;

- визначення критеріїв, яким має відповідати відкрите джерело інформації;
- дослідження правових аспектів отримання і використання інформації під час OSINT розслідувань;
- встановлення програмних засобів та інтелектуальних способів аналізу інформації з відкритих джерел;
- дослідження наявних відкритих джерел інформації, які можуть знадобитись у діяльності OSINT-розслідувача;
- визначення методології OSINT розслідування;
- дослідження процесу та існуючих етапів OSINT розслідування.

Після закінчення курсу здобувач повинен **знати**:
- визначення OSINT та суміжних категорій, які пов’язані із діяльністю щодо збору та аналізу інформації;
- зміст, хід та основні засоби, що застосовувались під час найактуальніших OSINT розслідувань;
- наявне коло інструментарію OSINT діяльності;
- критерії, яким має відповідати відкрите джерело інформації;
- правові аспекти отримання і використання інформації під час OSINT розслідувань;
- програмні засоби та інтелектуальні способи аналізу інформації з відкритих джерел;
- наявні відкриті джерела інформації, які можуть знадобитися у діяльності OSINT-розслідувача;
- методологію OSINT розслідування;
- процедуру та існуючі етапи OSINT розслідування.

Після закінчення відповідного курсу здобувач повинен **вміти**:
- надавати поняття OSINT та суміжних категорій, які пов’язані із діяльністю щодо збору та аналізу інформації;

- визначати зміст, хід та основні засоби, які застосовуються в конкретному OSINT розслідуванні;
- визначати необхідні інструменти для провадження ефективної OSINT діяльності;
- розрізняти відкриті джерела інформації від інших видів джерел;
- дотримуватись нормативно-правових аспектів отримання і використання інформації під час OSINT розслідувань;
- застосовувати програмні засоби та інтелектуальні способи для здійснення ефективного аналізу інформації з відкритих джерел;
- доцільно використовувати наявні відкриті джерела інформації, які можуть знадобитись у діяльності OSINT-розслідувача;
- ефективно використовувати методологію OSINT розслідування;
- планувати та в подальшому будувати процедуру та необхідні етапи OSINT розслідування.

Методи викладання і навчання передбачають використання мультимедійного обладнання та проведення практичних занять в спеціалізованих комп'ютерних класах за комп'ютерними робочими місцями для отримання та подальшої демонстрації практичних навичок пошуку інформації та роботи з нею.

Перелік тем практичних робіт:

Практичне заняття 1	Поняття, суміжні категорії OSINT. Історія, сфера застосування OSINT	2 години
Практичне заняття 2	Аналіз найактуальніших OSINT розслідувань	2 години
Практичне заняття 3	Джерела інформації для OSINT розслідувань	2 години
Практичне заняття 4	Відкриті бази даних – джерело для OSINT розслідувань	2 години

Практичне заняття 5	Інструменти OSINT розслідувань	2 години
Практичне заняття 6	Процес OSINT розслідувань	2 години
Практичне заняття 7	Правові аспекти отримання і використання інформації під час OSINT розслідувань	2 години

Перелік тем самостійної роботи:

Самостійна робота 1	Поняття, суміжні категорії OSINT. Історія, сфера застосування OSINT	8 години
Самостійна робота 2	Аналіз найактуальніших OSINT розслідувань	8 години
Самостійна робота 3	Джерела інформації для OSINT розслідувань	8 години
Самостійна робота 4	Відкриті бази даних – джерело для OSINT розслідувань	8 години
Самостійна робота 5	Інструменти OSINT розслідувань	8 години
Самостійна робота 6	Процес OSINT розслідувань	10 години
Самостійна робота 7	Правові аспекти отримання і використання інформації під час OSINT розслідувань	10 години

Правильність виконаних практичних і самостійних робіт перевіряє викладач.

Основними формами освітнього процесу є: лекційні, практичні заняття, консультування та самостійна робота здобувача.

Форми контролю: поточний та підсумковий (залік).

КРИТЕРІЇ ОЦІНЮВАННЯ ПІД ЧАС ПОТОЧНОГО КОНТРОЛЮ

Таблиця 1. Шкала оцінювання навчальної діяльності здобувача вищої освіти

Оцінка за шкалою силабусу	**Кількість набраних балів**	**Критерії оцінювання**
		Здобувач вищої освіти
A	90–100	виявив високу теоретичну підготовку, вміння аналізувати літературу, логічно та послідовно викладати фактичний матеріал, робити висновки. У процесі виконання практичної роботи чи аналізу поставлених завдань показує вміння планувати, ставити та інтерпретувати отримані результати відповідно до досягнень науки
B	82–89	виявив високий рівень теоретичних знань програмного матеріалу, вміння послідовно його викласти та застосувати засвоєні знання у процесі постановки і виконання практичної роботи, але допускає несуттєві неточності у відповідях, невеликі помилки у застосуванні теоретичних знань при виконанні практичних завдань
C	74–81	основному правильно висвітлив питання, але допускає несуттєві помилки у ході розв’язання завдань і показує задовільні знання теоретичного матеріалу
D	64–73	в основному правильно висвітлив питання, але допускає суттєві помилки у ході розв’язання завдань і показує задовільні знання теоретичного

		матеріалу
E	60–63	правильна, але неповна відповідь, яка свідчить про те, що здобувач вищої освіти вивчав матеріал, але не може логічно та повно висловити свою думку та застосувати його при виконанні практичних завдань

Тема 1. ПОНЯТТЯ, СУМІЖНІ КАТЕГОРІЇ OSINT. ІСТОРІЯ, СФЕРА ЗАСТОСУВАННЯ OSINT

Практичне заняття 1

1. Поняття OSINT, підходи до визначення.
2. Співвідношення OSINT з журналістськими розслідування.
3. Співвідношення OSINT з діяльністю розвідувальних органів.
4. Співвідношення OSINT з досудовим розслідуванням.
5. Історія формування OSINT.
6. Сфера застосування OSINT.
7. Засоби, що застосовуються під час OSINT.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно звернути увагу на наявність різних підходів до визначення поняття OSINT, що пояснюється відсутністю його нормативного закріплення. Важливо розуміти, що OSINT має різний масштаб його застосування. Так, він може бути лише окремим елементом в загальній, більш ширшій діяльності, або представляти собою окремий вид діяльності, який характеризується окремими, притаманними лише йому особливостями, які і відрізняють його з поміж інших.

Під час співвідношення OSINT з журналістським розслідуванням, діяльністю розвідувальних органів або ж досудовим розслідуванням, здобувачам необхідно використовувати наступні критерії: суб'єкти, які уповноважені на здійснення відповідної діяльності; засоби, які характерні та є легальними у кожному виді діяльності; відповідальність або ж ризики, на які наражаються особи, що здійснюють кожен вид зазначеної діяльності.

Важливим в процесі вивчення цієї теми є також дослідження історії OSINT в класичному її розумінні, історичних віх та подій які сприяли її розвитку, а також елементи OSINT діяльності в історії. Здобувачам необхідно також визначитись і з сферою застосування OSINT та можливими

обмеженнями цієї сфери. Для кращого розуміння OSINT діяльності варто приділити увагу засобам, що використовуються під час її провадження. При цьому бажано їх згрупувати, в залежності від родового об'єкта, а також вказати на ті засоби, що категорично заборонені для використання в OSINT діяльності, і ті, що можуть застосовуватись в окремих випадках.

Самостійна робота 1

Здобувачу необхідно надати відповідь на такі питання:

1. Які існують підходи до визначення OSINT?
2. Чим відрізняється вузьке від широкого розуміння OSINT діяльності?
3. Яким чином співвідносяться OSINT з журналістськими розслідування?
4. Що спільного у OSINT з діяльністю розвідувальних органів?
5. Як співвідносяться OSINT та досудове розслідування?
6. Які головні історичні віхи OSINT діяльності можна виділити?
7. Чи обмежена сфера застосування OSINT?
8. Які засоби, застосовуються під час OSINT діяльності та як розвиток соціуму і науково-технічного прогресу на це впливає?

Тема 2. АНАЛІЗ НАЙАКТУАЛЬНІШИХ OSINT РОЗСЛІДУВАНЬ

Практичне заняття 2

1. Критерії аналізу OSINT розслідувань.
2. Планування та загальний хід OSINT розслідування.
3. Засоби, що застосовувались OSINTерами.
4. Ризики, які існували під час OSINT розслідування.
5. Яким чином презентувались результати OSINT розслідування.
6. OSINT розслідування військової агресії проти України.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно зробити глибокий та змістовний аналіз запропонованого матеріалу щодо актуальних OSINT розслідувань. Так, окрім результатів розслідування та їх можливої інформаційної маніпуляції, необхідно проаналізувати запропоноване розслідування, за допомогою чітких критеріїв. Серед яких необхідно виділити наступні:

актуальність обраної теми та спонукання, які були в OSINTерів щодо її обрання;

планування здійснюваного розслідування;

засоби, що використовувались під час розслідування (важливо звернути на це увагу, оскільки в окремих випадках можливий вихід за межі OSINT діяльності);

час, який був витрачений на різні етапи OSINT діяльності, що сприятиме кращому розумінню розміру та інтенсивності зусиль, які необхідно прикласти для отримання бажаного результату;

яким чином здійснювалось планування розслідування та на які етапи воно було розділене;

які ризики або невдачі очікували OSINTерів та яким чином вони їх подолали;

як були презентовані результати OSINT розслідування чи є відповідний спосіб ефективним;

яких елементів або особливостей не вистачило під час здійснюваного OSINT розслідування.

Варто звернути увагу на наявні групи вітчизняних OSINTерів, які здебільшого працюють з інформацією щодо розслідування військової агресії проти України. В цьому контексті є важливим обрані напрямки розслідувань, конкретні засоби, що використовуються в однотипних видах розслідувань, час, який зазвичай витрачається для цього, і результати відповідних розслідувань та особливості використання отриманої інформації.

Самостійна робота 2

Здобувачу необхідно надати відповідь на такі питання:

1. Які OSINT розслідування для вас є взірцевими?
2. Які наявні критерії для здійснення аналізу OSINT розслідувань?
3. Яким чином планувалося та здійснювалося вами дослідження OSINT розслідування та які етапи воно в себе включало?
4. Які засоби використовувались під час досліджуваного OSINT розслідування; чи можна виокремити типові засоби для окремих видів OSINT розслідування?
5. Чи стикались OSINT розслідувачі із певними ризиками або негативними наслідками своєї діяльності; чи могли б вони потенційно мати місце?
6. Яким чином були презентовані результати OSINT розслідування, які наслідки вони мали; чи була досягнута мета, яка ставилась перед OSINTерами, на початку їх розслідування?
7. Яка роль сучасних OSINT розслідувань військової агресії проти України в сучасному військово-політичному вимірі?

Тема 3. ДЖЕРЕЛА ІНФОРМАЦІЇ ДЛЯ OSINT РОЗСЛІДУВАНЬ

Практичне заняття 3

1. Джерела OSINT розслідувань та їх критерії.
2. Види джерел інформації OSINT розслідувань за їх функціональним призначенням, офіційністю, достовірністю тощо.
3. Засоби масової інформації, оцінка їх контенту в якості інформації для OSINT розслідувань.
4. Соціальні мережі як джерело інформації. Особливості використання конфіденційної інформації, наявної у соціальних мережах.
5. Пошукові системи як джерело інформації.
6. Бази даних, види та використання їх як джерела інформації.
7. Сервіси з систематизації відкритої інформації про фізичних чи юридичних осіб.
8. Інтерв'ю осіб як джерело інформації для OSINT розслідування.

Методичні рекомендації

Під час дослідження питання джерел інформації для OSINT розслідувань здобувачам потрібно детальніше звернути увагу на ті джерела, які можна використовувати в OSINT діяльності, це або відкрита інформація, або ж джерела, які містять відкриту інформацію. У випадку використання інформації з обмеженим доступом, без наявності відповідного доступу до такого виду інформації, або знайомства з нею необмеженого кола осіб, які не мають відповідного доступу – зазначені дії, окрім явної невідповідності OSINT діяльності, тягнутимуть передбачену законом відповідальність, в тому числі кримінальну, що передбачено наступними статтями Кримінального кодексу України: 132 (розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби), 145 (незаконне розголошення лікарської таємниці), 168 (розголошення таємниці усиновлення (удочеріння)), частина 2

статті 201^9 (умисне порушення вимог законодавства про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення), 232 (розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках) тощо.

Особливістю відповідних джерел є те, що значна їх частина знаходиться в мережі Інтернет, і вони не мають класичного фізичного вираження. Це значно пришвидшує процес збору інформації, однак і формує певне перевантаження наявної інформації та потребує знань стосовно предмету пошуку, засобів для її сортування, а також знань щодо їх оперативної фіксації та збереження. Оскільки, у відповідній мережі з достатньо широкого кола джерел необхідно обрати ті, що будуть релевантні розслідуванню та будуть об'єктивними і не сфальсифікованими чи сфабрикованими.

Що ж стосується можливих видів джерел інформації OSINT розслідувань, то в залежності від різних критеріїв їх можна розподілити за функціональним призначенням, офіційністю, достовірністю, об'ємом наданої інформації, вартістю інформації, відношенням до об'єкту дослідження, законністю отримання тощо.

Найбільш розповсюдженим джерелом інформації є засоби масової інформації як в класичному друкованому вигляді, так і в електронному. Використовуючи їх, необхідно бути уважним, оскільки в останній час окремі ЗМІ стали засобом пропаганди. З огляду на це необхідно уважно досліджувати їх зміст як безпосередньо, так і в контексті з новинами інших джерел, і з подіями, що передували публікації. Також, варто звернути увагу і на формальні ознаки засобу масової інформації, такі як: репутацію видання, першоджерело з якого була взята інформація ; манера та об'єктивність її подання; правдивість та об'єктивність попередніх повідомлень конкретного ЗМІ.

Одним з найбільш сучасніших джерел інформації, яке є наслідком науково-технічного прогресу є соціальні мережі. Складність дослідження з них інформації полягає у їх значній кількості, що вимагає значного часу для пошуку профілю потрібної особи. Також складнощі у пошуку в соціальних мережах викликає зміна реальних відомостей особою в своєму профілі (наприклад використання логіну, який не відповідає імені та прізвищу особи). І звісно, особа може обмежити доступ до свого профілю чи сторінки, що вимагатиме від OSINTерів досконалого знання окремої соціальної мережі. Необхідно критично оцінювати наявну інформацію в соціальних мережах, оскільки особа через окремі бажання, обставин, цілі може дещо спотворювати надану інформації, фальсифікувати або навіть фабрикувати її. При цьому, варто звернути увагу на те, що соціальна мережа – яскравий приклад використання не відкритої інформації, а інформації, яка береться з відкритого джерела. Мається на увазі конфіденційна інформація щодо фізичної особи, яка в загальних умовах не підлягає розголошенню та використанню 3-ми особами, але факт її публікування в соціальній мережі самою особою, свідчить про дозвіл відповідної особи її використовувати іншими особами.

Нині існує значна кількість пошукових систем, які надають тисячі різних джерел інформації на запит. Для ефективного користування ними необхідно знати які комбінації варто вводити для пошуку інформації, а також переглядати не тільки першу сторінку із результатами пошуку інформації.

Для оптимізації державного управління та надання адміністративних послуг держава створює різні бази даних, яких налічується більше сотні. Зрозуміло, що до значної кількості з них обмежений доступ, але незважаючи на це, відкриті бази даних містять значний обсяг інформації, який може знадобитись особі під час її OSINT розслідування.

Одним із наслідків автоматизації та діджиталізації у суспільстві стали спеціалізовані Сервіси з систематизації відкритої інформації про фізичних чи юридичних осіб з відкритих джерел. Вони являють собою відкриті бази

даних, що дозволяє не витрачати час на дослідження кожної з них та оперативно отримати необхідну інформацію. Серед відповідних сервісів можна виділити YouControl та інші сервіси.

Також, варто виділити інтерв'ю або опитування осіб як джерело інформації для OSINT розслідування. Такий вид збору інформації є достатньо ефективним, що пояснюється можливістю оперативно уточняти у особи цікаві для розслідувача деталі. Разом з тим, на відміну від попередніх джерел, він пов'язаний із безпосереднім спілкуванням з особами, що в більшості випадків тягне за собою деанонімізацію OSINT аналітика, та може представляти певну небезпеку для OSINTера.

Самостійна робота 3

Здобувачу необхідно надати відповідь на такі питання:

1. Які вимоги ставляться до джерел, що можуть використовуватись під час OSINT розслідувань?
2. За якими критеріями можна систематизувати джерела OSINT розслідувань?
3. Які особливості роботи із засобами масової інформації як джерелами доказів?
4. Які складнощі можуть виникнути під час дослідження соціальних мереж в якості джерела інформації?
5. Які пошукові системи необхідно використовувати як джерело інформації та на що необхідно звернути увагу під час роботи з ними?
6. Що таке бази даних, в контексті OSINT розслідувань?
7. Які тактичні особливості роботи із сервісами щодо систематизації відкритої інформації про фізичних чи юридичних осіб?
8. Які переваги інтерв'ю та опитування осіб під час OSINT розслідування?

Тема 4. ВІДКРИТІ БАЗИ ДАНИХ – ДЖЕРЕЛО ДЛЯ OSINT РОЗСЛІДУВАНЬ

Практичне заняття 4

1. Відкриті бази даних, що засвідчують право власності осіб.
2. Відкриті бази даних, які направлені на запобігання корупційних діянь та контроль за державними посадовцями.
3. Відкриті бази даних, які містять інформацію про вартість майна.
4. Відкриті бази даних, що місять інформацію про земельні ділянки.
5. Відкриті бази даних, що містять інформацію про особу.
6. Відкриті бази даних, що містять судові рішення.
7. Відкриті даних, що містять довідкову інформацію.

Методичні рекомендації

Одними з найрозповсюдженіших джерел, які містять значний об’єм інформації – відкриті бази даних. В свою чергу, відкриті бази даних, що наявні у вітчизняному інформаційному просторі умовно можна поділити на наступні види: бази даних, що засвідчують право власності осіб; бази даних, які направлені на запобігання корупційних діянь та контроль за державними посадовцями; бази даних, які містять інформацію про вартість майна; бази даних, які містять інформацію про земельні ділянки; бази даних, що містять інформацію щодо окремих осіб; бази даних, які містять тексти судових рішень; бази даних, що містять довідкову інформацію.

Так, наприклад, до відкритих баз даних, що засвідчують право власності осіб можна віднести: Державний земельний кадастр, Державний реєстр речових прав на нерухоме майно. До відкритих баз, які направлені на запобігання корупційних діянь та контроль за державними посадовцями, необхідно віднести: Систему закупівель ProZorro, Єдиний державний реєстр декларацій, Єдиний державний реєстр осіб, які вчинили корупційні або пов’язані з корупцією правопорушення тощо. В свою чергу відкриті бази

даних, що містять інформацію про вартість майна це - Фонд державного майна (кабінет користувача єдиної бази даних звітів про оцінку), а також сервіси Державного земельного кадастру, за допомогою яких робиться нормативна грошова оцінка земельної ділянки та отримується інша інформація про земельну ділянку. До бази даних, яка містить особисту інформацію можна віднести інформаційну-аналітичну систему «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості». Що ж стосується баз даних, які містять судові рішення, то це Єдиний державний реєстр судових рішень, який має зручний інтерфейс для пошуку необхідної інформації за значною кількістю параметрів, а також база даних щодо стану розгляду справ, розміщена на сайті судової влади України. Що ж стосується баз даних, які містять довідкову інформацію, то до них необхідно віднести наступні: Антирейдерський союз підприємців України, Центр протидії корупції, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Автоматизована система виконавчого провадження тощо.

Додатково необхідно зауважити, що для доступу до значної частини з цих баз даних особі знадобиться або авторизація за допомогою BankID або за допомогою КЕП, з огляду на це – в особи має бути відповідний інструментарій.

Самостійна робота 4

Здобувачу необхідно надати відповідь на такі питання:

1. Наведіть приклади баз даних, що засвідчують право власності осіб?
2. Які бази даних направлені на запобігання корупційних діянь та здійснення контролю за державними посадовцями?
3. Які з відомих вам баз даних містять довідкову інформацію?
4. Які бази даних містять інформацію про вартість майна?

5. Яку інформацію про земельну ділянку можна отримати за наслідками роботи з Державним земельним кадастром?

6. Яку особисту інформацію можна отримати з відкритих державних баз даних?

7. В якій базі даних зібрані рішення українських судів?

Тема 5. ПРОЦЕДУРА OSINT РОЗСЛІДУВАНЬ

Практичне заняття 5

1. Обрання напрямку дослідження: критерії, мета, задачі.
2. Початковий етап OSINT розслідування.
3. Збір інформації як етап OSINT розслідування.
4. Аналіз зібраної інформації, її перевірка.
5. Висновки за наслідками OSINT розслідування.
6. Розповсюдження, презентація висновків OSINT розслідування.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на необхідності системного підходу для здійснення OSINT розслідувань, що забезпечить ефективне використання наявних в особи ресурсів та значно підвищить можливості для отримання бажаних результатів. Процес OSINT розслідування бажано розділити на наступні ключові етапи: обрання напрямку розслідування, початковий етап, збір інформації, аналіз та перевірка зібраної інформації, формування висновків та розповсюдження висновків проведеного дослідження.

Під час обрання напрямку OSINT дослідження, окрім можливої актуальності або цікавості безпосередньо особі, необхідно звернути увагу чи не стосується обрана тема інформації з обмеженим доступом, чи наявні відкриті джерела інформації, чи відкрита інформація стосовно відповідної тематики, чи вистачить у особи ресурсів для проведення дослідження з відповідної тематики. Під час цього етапу особа має чітко визначити стратегічні цілі своєї діяльності та усвідомлювати реальність їх досягнення.

Початковий етап представляє собою інтелектуально-оціночну діяльність, яка направлена на деталізацію до тактичного рівня визначених стратегічних цілей та на планування OSINT розслідування. Під час нього особі необхідно визначитись із чітким переліком дій, що треба вчинити,

можливими джерелами інформації, які будуть досліджуватись, орієнтовним часом, який буде витрачатись під час вчинення кожної із дій.

Збираючи інформацію, особа має усвідомлювати, що тип джерела та самої інформації, які використовуються - мають бути відкритими та не відноситись до інформації з обмеженим доступом, в протилежному випадку OSINT дослідження може трансформуватись в діяльність, за провадження якої передбачена юридична відповідальність. Серед особливостей відповідного етапу необхідно виділити наступні: необхідність використовувати значну кількість джерел (чим більше тим краще), необхідність попереднього аналізу інформації для її фільтрації, фіксації чи збереження саме на етапі ознайомлення з нею. Важливими, в цьому контексті, є знімки екрану та завантаження цікавого OSINTеру контенту, а не тільки збереження відповідних посилань, це унеможливить в подальшому негативні наслідки для розслідувача у випадку фальсифікації, зміни інформації або її видалення.

Аналіз зібраної інформації бажано має відбуватись із залученням особи, яка є спеціалістом у досліджуваному масиві даних, окрім оперативності це дозволить уникнути можливих неточностей чи помилок під час аналізу зібраної інформації. Важливим є також перевірка наявних даних, особливо, якщо отримана інформація, з різних джерел, різниться, в такому випадку пріоритет має надаватись інформації з більш надійного джерела або ж у висновках до розслідування необхідно про це зазначити. Аналіз є найбільш часозатратним етапом, оскільки отримана інформація має перевірятися змістовно, структурно, має оцінюватись джерело її походження, час публікації тощо.

Висновки за наслідками OSINT розслідування можуть бути представлені в двох формах: чіткі твердження або відсутність певного твердження, однак наявність чи констатація сукупності фактів чи аргументів, які дозволяють особам, що з ними знайомляться зробити висновки самостійно. Відповідна форма має обиратись в залежності від виду

розслідування, його об’єкту, піднятої теми, юридичних наслідків, сформованих чітких висновків тощо. Під час формування висновків, необхідно використовувати аргументацію, тобто посилання на інформацію, яка про них свідчить, та на джерела відповідної інформації (які мають бути авторитетними, об’єктивними та правдивими, особливо в контексті наявної пропаганди та інформаційних війн в медіа). Важливим є також формування висновків, внаслідок саме усестороннього дослідження об’єкта дослідження, що свідчитиме про його об’єктивність та неупередженість.

Наступним етапом OSINT розслідування після формування висновків є їх презентація та розповсюдження, оскільки як і будь-який вид діяльності OSINT у підсумку має впливати на навколишнє середовище та оточуючих. Відповідний етап можна розподілити на окремі види в залежності від публічності презентації результатів OSINT розслідування: на публічні, з обмеженим доступом та індивідуальні. А також в залежності від суб’єктів, яким відповідні висновки презентуються: громадськості (необмеженому колу осіб), працівникам правоохоронних органів (іноді у формі повідомлення про вчинення кримінального правопорушення), військовим формуванням, керівникам державних чи приватних структур або окремим особам.

Самостійна робота 5

Здобувачу необхідно надати відповідь на такі питання:

1. Які критерії для обрання тематики OSINT розслідування?
2. Які задачі вирішуються на першому етапі OSINT розслідування, присвяченому обранню напрямку дослідження?
3. Які дії необхідно вчинити на початковому етапі OSINT розслідування?
4. Які особливості збору інформації як етапу OSINT розслідування?
5. В чому полягає аналіз зібраної інформації як етапу OSINT розслідування?

6. Для чого необхідно перевіряти зібрану інформацію під час OSINT дослідження?

7. Яким чином можна формулювати висновки за наслідками OSINT розслідування?

8. Кому можуть бути презентовані висновки OSINT розслідування та з якою метою?

Тема 6. ІНСТРУМЕНТИ OSINT РОЗСЛІДУВАНЬ

Практичне заняття 6

1. Інструменти для покращення зображення.
2. Інструменти для визначення місцезнаходження об’єктів.
3. Інструменти для виявлення редагування зображення.
4. Інструменти для аналізу сайту.
5. Метадані як інструмент для OSINT аналітика.
6. Сервіси викраденого майна та недійсних документів.
7. Штучний інтелект та його використання в якості помічника під час OSINT розслідувань.
8. Інші інструменти, що оптимізують роботу OSINTерів.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на наявність інструментарію для роботи з інформацією в різних її формах. Здебільшого інструменти OSINT розслідування представлені різним програмним забезпеченням, з огляду на що їх кількість постійно збільшується, разом із умовами їх використання, на що необхідно звертати увагу OSINTерам для постійного пошуку більш досконалого інструментарію та більш прийнятних умов їх використання.

Так, серед ***інструментів для покращення зображення можна виділити наступні***:

- **Fixblur**

- **Imglarger**

Що ж стосується ***інструментів для визначення місцезнаходження***

***об'єктів, то їх умовно можна поділити на різні види*:**

- ***інструменти, які містять топографічні карти, супутникові зніми та фото місцевості***:

- **GISFile**

- **Google maps**
- **Soar** (атлас з картами, супутниковими знімками. В тому числі, історичні карти, кліматичні, агрокультури, геологія, транспортні, морські, змін навколишнього середовища, рельєфів)

- ***інструменти для пошуку місця, де могла бути зроблена фотографія:***

- **Shadow Finder** (Надає можливі варіанти місць, де була зроблена фотографія, для цього вимірюється об'єкт, та його тінь на зображені (одиниці вимірювання неважливі, ключовими є пропорції) у випадку, якщо відома дата та час фотозйомки. Зазначені вище дані (пропорції, час та дата) вносяться у програму, яка і розраховує всі можливі місця, де могла бути така тінь в той момент, дослідити залишається лише запропоновані місця.

- **SunCalc** (сонячний календар, функціонал якого дозволяє визначати тінь об'єкта, знаючи його висоту в конкретному місці в конкретну дату і час та навпаки. А також, знаючи

пропорції висоти об’єкта та його тіні, та місце його фіксування – визначити час і дату фіксування.

● **Image Measurement** та **Scale fixereng** (автоматично розраховують розміри об’єктів на фотографіях, для цього достатньо вказати розмір хоча б одного з них)  та

Серед ***інструментів для виявлення можливого редагування зображення, можна виділити наступні:***

● **Forensically** та **Maver** (призначені для виявлення можливих слідів редагування на фото. Працюють тільки з оригіналами фото)

 та 

● **Source Searcher** – (бот в Telegram для пошуку звідки було взято фотографію в Інтернеті).

● **AI or not** – відповідний інструмент дозволяє визначитись чи створювалось фото внаслідок використання можливостей штучного інтелекту.

- **DeepWare** – інструмент, який перевіряє чи не має слідів заміни обличчя, голосу або міміки у відео.

Серед ***інструментів, які аналізують сайт можна виділити наступні***:

- **Website OSINT** (список ресурсів, які допомагають при дослідженні або аналізі веб-сайтів, а саме в пошуку сайтів, які належать одній особі, домени з однаковим ідентифікатором Google Adsense ID, які технології стеження, фрейм ворки та віджети використовуються і куди витікають дані користувачів, архіви тощо)

Характеризуючи ***метадані як інструмент для OSINT аналітики***, необхідно зазначити, що в найбільш загальному визначенні метадані – це дані про дані. Тобто звичайне фото окрім безпосередньо зображення має містити інформацію щодо часу та дати його створення, його джерело, можливо навіть місця фотографування. Серед наявних інструментів, які дозволяють працювати з метаданими можна виділити наступні: онлайн-сервіси, які добувають метадані з різних мультимедійних файлів:

- **EXIFtool**
- **Metadata2go**

Цікавими в контексті OSINT ***дослідження є сервіси з відображення***

викраденого майна та недійсних документів:

- **Перевірка недійсних документів (**Державна міграційна служба**)**

- **Сервіси МВС (**в тому числі щодо викрадених телефонів чи транспортних засобів, зниклих осіб, зброї, що знаходиться у розшуку**)**

OSINT розслідування характеризуються активним використанням досягнень науково-технічного прогресу у своїй діяльності. Штучний інтелект не став виключенням та активно використовується OSINT аналітиками у своїй діяльності, серед відповідних інструментів необхідно виділити наступні:

- **Search Whisperer** (гугл доркінг зі штучним інтелектом. Самостійно перефразовує запити, щоб покращити результат видачі. Складає пошукові запити замість користувача)

- **Lenso** (інструмент зворотного пошуку зображень на базі ШІ. Представляє собою модифіковану версію пошуку за фото від Google та Bing, але зі зручнішим сортуванням. Доречний для пошуку схожих локацій, об'єктів або людей)

Наведені нами інструменти, що оптимізують роботу OSINTерів не є вичерпними і складають лише незначну частину від загальної кількості

інструментарію, який може використовуватись для роботи та збільшення ефективності під час OSINT розслідування. Так, серед інших видів можна виділити наступний інструментарій:

- **Epieos** (інструмент, що здійснює пошук за електронною поштою. Надає інформацію щодо Google акаунту (ID, фото, прив'язку до Google maps, календаря тощо), Skype, та наявності інших соц. мереж і сервісів, пов'язаних з поштою)

- **Кібербез** (канал в Telegram, який активно оновлює інформацію щодо активних інструментів та методів OSINT розслідування, разом з їх описами, відео щодо користування ними та прикладами безпосереднього використання в OSINT діяльності)

Самостійна робота 6

Здобувачу необхідно надати відповідь на такі питання:

1. Які наявні інструменти для покращення зображення?
2. Які сервіси краще використовувати для визначення місцезнаходження об'єктів?
3. За допомогою яких програмних засобів можна виявити редагування зображення або відео?
4. Якими інструментами можна проаналізувати сайт?
5. Яку роль метадані відіграють у OSINT розслідуванні?
6. За допомогою яких сервісів можна дослідити метадані окремих файлів?
7. Які наявні інструменти для перевірки викраденого майна та недійсних документів?

8. Які наявні напрями використання штучного інтелекту під час OSINT розслідування

Тема 7. ПРАВОВІ АСПЕКТИ ОТРИМАННЯ І ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПІД ЧАС OSINT РОЗСЛІДУВАНЬ

Практичне заняття 7

1. Види інформації відповідно до Закону України «Про інформацію».
2. Особливості використання інформації відповідно до Закону України «Про інформацію».
3. Протокол Берклі, поняття та загальна характеристика.
4. Методичні вказівки протоколу Берклі щодо перевірки отриманої інформації для здійснення розслідування.
5. Способи отримання відкритих цифрових даних відповідно до протоколу Берклі.
6. Відмінність між доказом та інформацією згідно із протоколом Берклі.
7. Засади отримання інформації згідно із протоколом Берклі.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на положення Закону України «Про інформацію». Здобувачі мають приділити увагу поняттю інформація, яке закріплене у відповідному законі, суб'єктам та об'єктам інформаційних відносин. Детально необхідно переглянути види інформації за змістом, яку нам пропонує зазначений нормативно-правовий акт: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; критична технологічна інформація та інші види інформації.

Окремо необхідно дослідити види інформації за порядком доступу, серед яких законодавець виділяє відкриту інформацію та інформацію з

обмеженим доступом, яку в свою чергу поділяє на конфіденційну, таємну та службову інформацію. Важливим в цьому контексті є також ознайомлення із нормами Закону України «Про інформацію», які присвячені можливій відповідальності за порушення законодавства про інформацію та випадки звільнення особи від відповідальності за вказані порушення.

Досліджуючи Протокол Берклі, здобувачі мають розуміти, що відповідний документ не є нормативним, і носить лише рекомендаційний характер. Оскільки він був сформований як навчальний посібник в якості набору глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях щодо порушення прав людини. Його положення окрім тактичних особливостей збирання інформації, акцентують увагу і на формі збирання, закріплення та перевірки доказів, що в подальшому сприятиме забезпеченню можливості їх використання.

Так, що стосується методичних вказівок стосовно перевірки отриманої інформації для здійснення розслідування протокол Берклі акцентує увагу на необхідності:

- відстеження походження онлайн-контенту та по можливості вказівки його першоджерела;
- оцінки достовірності та надійності онлайн-джерел; перевірки онлайн-контенту та оцінки його істинності та надійності;
- дотримання вимог законодавства та етичних норм;
- мінімізації будь-якого ризику заподіяння шкоди собі, своїм організаціям та третім особам;
- посилення захисту прав людини джерел, включаючи право на недоторканність приватного життя.

Що ж стосується можливих способів отримання відкритих цифрових даних, то протокол Берклі виділяє наступні: спостереження; запит; придбання інформації; розвіддані з відкритих джерел. В свою чергу у Протоколі зазначається, що термін «доказ» слід відрізняти від терміна «інформація».

Докази визначаються як підтвердження факту (фактів), що використовується у розслідуванні або подані до суду. Відкриті дані як доказ — це інформація з відкритих джерел, яка має доказову силу і може бути прийнята для встановлення фактів під час судового розгляду. Під час розслідування або представлення результатів, важливо не зловживати терміном «доказ» та не використовувати його надмірно, коли йдеться про «інформацію» загалом. В свою чергу докази мають відповідати наступним критеріям: достовірність (правдоподібність чи переконливість), надійність (здатність робити щось послідовно, стабільно, що відповідає очікуванням) та істинність (точність, правильність, відповідність до фактів).

Досліджуючи засади отримання інформації згідно із протоколом Берклі, необхідно виділити наступні:

- законність;
- знання та розуміння заходів безпеки;
- відповідальність;
- об’єктивність;
- компетентність.

Самостійна робота 7

Здобувачу необхідно надати відповідь на такі питання:

1. Які є види інформації за змістом відповідно до Закону України «Про інформацію»?
2. Які види інформації за порядком доступом до неї виділяє Закону України «Про інформацію»?
3. Які особливості використання інформації відповідно до Закону України «Про інформацію»?
4. Яка можлива відповідальність передбачена за порушення законодавства України про інформацію?

5. В яких випадках передбачено звільнення від відповідальності за порушення порядку доступу до інформації?

6. Поняття та загальна характеристика Протоколу Берклі.

7. Методичні вказівки протоколу Берклі щодо перевірки отриманої інформації для здійснення розслідування.

8. Способи отримання відкритих цифрових даних відповідно до протоколу Берклі.

9. Відмінність між доказом та інформацією згідно із протоколом Берклі.

10. Засади отримання інформації згідно із протоколом Берклі.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ

1. В чому полягає аналіз зібраної інформації як етап OSINT розслідування.
2. В яких випадках передбачено звільнення від відповідальності за порушення порядку доступу до інформації.
3. В якій базі даних зібрані рішення українських судів.
4. Види інформації за змістом відповідно до Закону України «Про інформацію».
5. Відмінність між доказом та інформацією згідно із протоколом Берклі.
6. Для чого необхідно перевіряти зібрану інформацію під час OSINT дослідження.
7. За допомогою яких програмних засобів можна виявити редагування зображення або відео.
8. За допомогою яких сервісів можна дослідити метадані окремих файлів.
9. За якими критеріями можна систематизувати джерела OSINT розслідувань.
10. За якими критеріями можна систематизувати джерела OSINT розслідувань.
11. Засади отримання інформації згідно із протоколом Берклі.
12. Кому може бути презентовані висновки OSINT розслідування та з якою метою.
13. Методичні вказівки протоколу Берклі щодо перевірки отриманої інформації для здійснення розслідування.
14. Наведіть приклади баз даних, що засвідчують право власності осіб.
15. Наведіть приклади відкритих джерел, що засвідчують право власності осіб.

16. Поняття та загальна характеристика Протоколу Берклі.

17. Способи отримання відкритих цифрових даних відповідно до протоколу Берклі.

18. Чи існує відповідальність за OSINT розслідування.

19. Чи обмежена сфера застосування OSINT.

20. Чи стикались OSINT розслідувачі із певними ризиками або негативними наслідками своєї діяльності чи могли б вони потенційно мати місце.

21. Чим OSINT розслідування відрізняється від діяльності розвідувальних органів.

22. Чим OSINT розслідування відрізняється від досудового розслідування.

23. Чим OSINT розслідування відрізняється від журналістського розслідування.

24. Чим відрізняється вузьке від широкого розуміння OSINT діяльності.

25. Що спільного у OSINT з діяльністю розвідувальних органів.

26. Що таке бази даних, в контексті OSINT розслідувань.

27. Як співвідносяться OSINT та досудове розслідування.

28. Яка можлива відповідальність передбачена за порушення законодавства України про інформацію.

29. Яка роль сучасних OSINT розслідувань військової агресії проти України в сучасному військово-політичному вимірі.

30. Яким чином були презентовані результати OSINT розслідування, які наслідки вони мали; чи були досягнута мета, яка ставилась перед OSINTерами на початку їх розслідування.

31. Яким чином можна формулювати висновки за наслідками OSINT розслідування.

32. Яким чином плануються, здійснюються досліджувані вами OSINT розслідування та які етапи вони в себе включають.

33. Яким чином співвідноситься OSINT з журналістськими розслідування.

34. Якими інструментами можна проаналізувати сайт.

35. Які OSINT розслідування для вас є взірцевими.

36. Які бази даних містять інформацію про вартість майна.

37. Які бази даних направлені на запобігання корупційних діянь та здійснення контролю за державними посадовцями.

38. Які види інформації за порядком доступом до неї виділяє Закону України «Про інформацію».

39. Які вимоги ставляться до джерел, що можуть використовуватись під час OSINT розслідувань.

40. Які відкриті джерела, направлені на запобігання корупційних діянь та здійснення контролю за державними посадовцями.

41. Які головні історичні віхи OSINT діяльності можна виділити.

42. Які дії необхідно вчинити на початковому етапі OSINT розслідування.

43. Які з відомих вам баз даних містять довідкову інформацію.

44. Які з відомих вам відкритих джерел містять довідкову інформацію.

45. Які задачі вирішуються на першому етапі OSINT розслідування, присвяченому обранню напрямку дослідження.

46. Які засоби використовувались під час досліджуваного OSINT розслідування чи можна виокремити типові засоби для окремих видів OSINT розслідування.

47. Які засоби застосовуються під час OSINT діяльності та як розвиток соціуму і науково-технічного прогресу на це впливає.

48. Які існують підходи до визначення OSINT.

49. Які критерії для обрання тематики OSINT розслідування.

50. Які наявні інструменти для перевірки викраденого майна та недійсних документів.

51. Які наявні інструменти для покращення зображення.

52. Які наявні критерії для здійснення аналізу OSINT розслідувань.

53. Які наявні напрями використання штучного інтелекту під час OSINT розслідування.

54. Які особливості використання інформації відповідно до Закону України «Про інформацію».

55. Які особливості збору інформації як етапу OSINT розслідування.

56. Які особливості роботи із засобами масової інформації як джерелами доказів.

57. Які переваги інтерв'ю та опитування осіб під час OSINT розслідування.

58. Які пошукові системи необхідно використовувати як джерело інформації та на що необхідно звернути увагу під час роботи з ними.

59. Які сервіси краще використовувати для визначення місцезнаходження об'єктів.

60. Які складнощі можуть виникнути під час дослідження соціальних мереж, в якості джерела інформації.

61. Які тактичні особливості роботи з сервісами з систематизації інформації про фізичних чи юридичних осіб.

62. Яку інформацію про земельну ділянку можна отримати за наслідками роботи з Державним земельним кадастром.

63. Яку особисту інформацію можна отримати з відкритих державних баз даних.

64. Яку роль метадані відіграють у OSINT розслідуванні.

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

Нормативно-правові акти

1. Загальні рекомендації Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку для підвищення рівня захисту інформаційних ресурсів та систем і для запобігання кіберінцидентам в установах, на підприємствах і в організаціях. URL: https://www.kmu.gov.ua/news/250099405

2. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575

3. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року, № 1009-р. URL: http://zakon2.rada.gov.ua/laws/show/1009-2017-р

4. Кримінальний кодекс України від 05 квітня 2000 року, № 2341III. URL: https://zakon.rada.gov.ua/laws/show/234114#n89

5. Кримінальний процесуальний кодекс України від 13 квітня 2012 року, № 4651VI. URL: https://zakon.rada.gov.ua/laws/show/465117#Text

6. Питання діяльності Міністерства інформаційної політики України : Постанова Кабінету Міністрів України від 14.01.2015 № 2. Офіційний вісник України. 2015. № 6. С. 124

7. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. *Рада національної безпеки і оборони України*. URL: https://zakon.rada.gov.ua/laws/show/32/2017

8. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 року, № 518. Офіційний вісник України від 02.07.2019. 2019. № 50. С. 53. Стаття 1697, код акту 94896/2019

9. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету міністрів України від 29 березня 2006 року, № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

10. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року, № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

11. Про захист персональних даних : Закон України від 01 червня 2010 року, № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

12. Про звернення громадян: Закон України від 02 жовтня 1996 року, № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text

13. Про інформацію: Закон України від 02 жовтня 1992 року, № 2657-XII / Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12

14. Про національну безпеку України : Закон України від 21 червня 2018 року, № 2469-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19/print1509543369819103

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

16. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32»: Рішення РНБО від 10 липня 2017 року. *Рада національної безпеки і оборони України*. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17#Text

17. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 року, № 96/2016. *Президент України*. URL: https://www.president.gov.ua/documents/962016-19836

18. Стратегія кібербезпеки України: Указ Президента України від 14 травня 2021 року, № 447/2021. *Президент України*. URL: https://www.president.gov.ua/documents/4472021-40013

19. Цивільний кодекс України: Кодекс України від 16 січня 2003 року, № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Tex

Основні джерела

1. Açar, K.V. (2018). OSINT by Crowd-Sourcing: *A Theoretical Model for Online Child Abuse Investigations/ International Journal of Cyber Criminology*. Vol. 12(1): 206–229.1467897 Publisher & Editor-in-Chief. K. Jaishankar

2. Heather J. Williams, Ilana Blum. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Library of Congress Control Number: 2018943942

3. NATO Open Source Intelligence Handbook, November 2001. URL: http://www. oss.net/dynamaster/file_archive/030201/ca5 fb66734f540fbb4f8f6ef759b258c/NATO%20 OSINT%20Handbook%20v1.2%20- %20 Jan%202002.pdf

4. Nihad A. Hassan, Rami Hijazi. (2018). Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence

5. Office of the Director of National Intelligence, "What is Intelligence?," 24 May 2017, https://www.dni.gov/index.php/what-we-do/what-is-intelligence

6. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. URL: www.fas.org/sgp/crs/intel/RL34270.pdf

7. Open Source Intelligence, U.S. Army Field Manual Interim FMI 2-22.9, December 2006. URL: www.fas.org/irp/doddir/army/fmi2-22-9.pdf

8. OSINT (воєнна розвідка відкритих джерел) в екосистемі зв`язаних термінів. URL: https://dss-bi.blogspot.com/2019/01/osint.html

9. Richard Holt, “Twitter in Numbers,” Telegraph, 21 March 2013, http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.htm

10. The Big Data Imperative. Air Force Intelligence for the Information Age. Air & Space Power Journal, 2018/2/11 Col Shane P. Hamilton, USAF; Lt Col Michael P. Kreuzer, USAF, PhD

11. Адаптація розвідки НАТО для підтримки «Єдиної НАТО». URL: https://www.nato.int/docu/ review/uk/articles/2017/09/08/adaptatsya-rozvdkinato-dlya-pdtrimki-dino-nato/index.html

12. Бердинских Х. Заборона російських соціальних мереж – це безпека країни чи обмеження демократичних свобод. URL: https://24tv.ua/zaborona_rosiyskih_sotsialnih_merezh__tse_bezpeka_krayini_chi_ obmezhennya_demokrati chnih_svobod_n819269

13. Бойовий OSINT. Розбираємо сучасні методи розвідки мережі. URL: https://www. guardianelinks.com/threads/boevoj-osint-razbiraemsovremennye-metody-setevoj-razvedki.38215

14. Бурба В.В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. *Юридичний бюлетень* 2019. № 11, Ч. 1. С. 11-19

15. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. *Інформаційна безпека*: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с.

16. В Україні набув чинності указ про блокування ВКонтакте і Одноклассников. URL: https://www.unian.ua/ politics/1926399-v-ukrajini-nabuv-chinnosti-ukaz-pro-blokuvannya-vkontakte-i-odnoklassnikov.html

17. Васюк К. В. Автоматизація збору корпоративної та особистої інформації з відкритих джерел : кваліфікаційна робота бакалавра за спеціальністю „125 кібербезпека“. Тернопіль. 2021. 73 с.

18. Власенко В. Генсек Ради Європи: Блокування соціальних мереж не відповідає принципу свободи ЗМІ. URL: http://p.dw.com/p/2d5iH

19. Войціховський, А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*, 2020. № 29. С. 281-288. https://doi.org/10.26565/2075-1834-2020-29-38

20. Гнусов Ю.В., Кійков В.М. Сучасні тенденції розвитку DDoS-атак. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

21. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І.Г. Грабар, Р.В. Грищук, К.В. Молодецька. Житомир : ЖНАЕУ, 2019. 280 с.

22. Дикий О.В., Сидорчук В.В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал.* 2024, № 9. С.332-336. DOI: https://doi.org/10.32782/2524-0374/2024-9/78

23. Дуцик Д. Інформаційний вакуум: як українські телеканали висвітлюють події на Донбасі та в Криму. URL: https://hromadskeradio.org/programs/kyiv-donbas/informaciynyy-vakuum-yak-ukrayinski-telekanalyvysvitlyuyut-podiyi-na-donbasi-ta-v-krymu

24. Еделєва М.А. Забезпечення інформаційної безпеки в контексті реалізації державної інформаційної політики. *Вісник Маріупольського державного університету. Серія «Історія. Політологія».* 2017. Вип. 19. С. 133–141

25. Жарков Я.М., Васильєв А.О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник національного університету імені Тараса Шевченка.* 2013. Вип. 30. С. 38-41

26. Жарков Я. М. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 38-41

27. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. *Соціально-правові студії* : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 3 (9). С. 18–25

28. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис.* 2016. № 2. С. 110-113

29. Карпенко А.О., Мусієнко В.А., Шугалій О.О., Пономаренко З.М. Аналіз інструментів збору розвідувальної інформації з відкритих джерел. *Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи*. Київ: ВІТІ, 2022. № 1 (3). С. 18-25

30. Козюра В.Д., Хорошко В.О. Як протистояти реальним кіберзагрозам об’єктам критичної інфраструктури України. *Кібербезпека в Україні*: правові та організаційні питання : матеріали Всеукр. наук.- практ. конф., м. Одеса, 17 листопада 2017 р. Одеса : ОДУВС, 2017. С. 79–80

31. Лук’янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України. Сер.: Державне управління*. 2016. № 3. С. 131-137

32. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* 2021. № 9. С. 332-334. URL: http://www.lsej.org.ua/9_2021/85.pdf

33. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв’язку*. 2016. Вип. 4. С. 81–84. URL: http://nbuv.gov.ua/UJRN/suntz2016422

34. Пащенко Т. П. Гібридна війна та соціальні мережі. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62-65

35. Пащенко Т. П. Гібридна війна та соціальні мережі. *Інформаційний вимір гібридної війни*: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62–65

36. Присяжнюк М. М., Бєлошевич Я. С. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 37–41

37. Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE). *Україна в системі глобального інформаційного обміну*: теоретико-методологічні аспекти дослідження і підготовки фахівців : всеукраїнська наукова конференція, Львів, 27 травня 2011 р. / Національний університет "Львівська політехніка". – Львів : Видавництво Львівської політехніки, 2011. – С. 257–261 URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content

38. Світличний В.А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем. *Кібербезпека в Україні*: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88–89

39. Світличний В.А., Петров К.Е. Від ідентифікації комп'ютера до ідентифікації користувача у мережі Інтернет. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

40. Серватнюк М. Інтеграція методів OSINT в систему управління інформаційним ризиками. ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ : IX науково-техн. конф., м. Тернопіль, 8–9 груд. 2021 р. 2021. с. 76

41. Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. *Збірник наукових*

праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. 2018. Вип. № 3. С. 56–66

42. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник / О.О. Торбас. - Одеса : Видавництво «Юридика», 2024. – 180 с.

43. Торяник В.В., Чмирь А.Ю. Актуальність проблеми атаки на відмову в обслуговуванні. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.- практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

44. Трофименко О.Г., Логінова Н.І., Манаков С.Ю., Янковський О.Г. Кіберризики в освітньому секторі. *Сучасна спеціальна техніка.* 2022, №2. С. 111-117 Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/ research_reports/RR1964.html

45. Яровой Т.С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління.* 2019. № 4 (6). С. 201-208

46. Яфонкін А. О. Обіг неправдивої інформації у засобах масової комунікації в Україні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2017. Вип. 2–3 (6–7). С. 153–158

47. Яфронін А.О., Шевчук В.А. Інформаційна війна проти держави та інформаційна безпека України. *Форум права.* 2017. № 5. С. 466-472. URL: http://forumprava.pp.ua/files/466-472-2017-5----------,--------73-.pdf

Додаткові джерела

1. Açar, K.V. (2018). OSINT by Crowd-Sourcing: *A Theoretical Model for Online Child Abuse Investigations/ International Journal of Cyber*

Criminology. Vol. 12(1): 206–229.1467897 Publisher & Editor-in-Chief. K. Jaishankar

2. Domingues V. Finance and Cybersecurity Risk Management: Dissertation. 2018. 51 p. URL: https://www.researchgate.net/publication/344711134_Finance_and_ Cybersecurity_Risk_Management

3. Dorothy E. Denning (May 23, 2000). “Cyberterrorism”. cs.georgetown.edu. Archived from the original on March 10, 2014. Retrieved June 19, 2016

4. Jureviciene A., Brilingaite A., Bukauskas L. Digital Human in Cybersecurity Risk Assessment. HCII 2021. Lecture Notes in Computer Science. 2021. Vol 12776. Springer, Cham. DOI: https:// doi.org/10.1007/978-3-030-78114-9_29. URL: https://link.springer.com/chapter/10.1007%2F978-3- 030-78114-9_29#citeas

5. Naidoo R. A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems. 2020. Vol. 29(3). P. 306-321. DOI: 10.1080/0960085x.2020.1771222

6. Savchenko V., Matsko O. Cybersecurity risk management on the basis of game-theoretic approach. Modern information security. 2019. Vol. 2(38). P. 6-16. DOI: 10.31673/2409-7292. 2019.020616

7. UlvenJ., Wangen G. A Systematic Review of CybersecurityRisks in Higher Education. Future Internet. 2021. Vol. 13. 39 p. DOI: 10.3390/fi13020039. URL: https://www.researchgate.net/publication/

8. Williams Ch., Chaturvedi R., Chakravarthy K. Cybersecurity Risks in a Pandemic. Journal of Medical Internet Research. 2020. Vol 22. DOI: 10.2196/23692. URL: https://wwwjmir.org/2020/9/ e23692/

9. Бердинских Х. Заборона російських соціальних мереж – це безпека країни чи обмеження демократичних свобод. URL: https://24tv.ua/zaborona_rosiyskih_sotsialnih_merezh__tse_bezpeka_krayini_chi_ obmezhennya_demokrati chnih_svobod_n819269

10. Бойовий OSINT. Розбираємо сучасні методи розвідки мережі. URL: https://www. guardianelinks.com/threads/boevoj-osint-razbiraemsovremennye-metody-setevoj-razvedki.38215

11. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

12. Дуцик Д. Інформаційний вакуум: як українські телеканали висвітлюють події на Донбасі та в Криму. URL: https://hromadskeradio.org/programs/kyiv-donbas/informaciynyy-vakuum-yak-ukrayinski-telekanalyvysvitlyuyut-podiyi-na-donbasi-ta-v-krymu

13. Жарков Я. М. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 38-41

14. Жмур Н.В., Землянікіна М.П. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Юридичний вісник*. 2022, № 3 (64). С.95-101

15. Карпенко А.О., Мусієнко В.А., Шугалій О.О., Пономаренко З.М. Аналіз інструментів збору розвідувальної інформації з відкритих джерел. Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. Київ: ВІТІ, 2022. № 1 (3). С. 18-25

16. Кіберзлочинність – загроза банківській системі. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vnbu_2015_4_7.pdf

17. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. *Науковий вісник*. 2011. № 4, Том 2. С. 68-74

18. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. Київ : ВІКНУ, 2016. 286 с.

19. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Київ, 2005. 20 с.

20. Мандзюк О.А. Роль аналітичної діяльності та аналітичних центрів у формуванні й реалізації кібербезпекової політики. URL: http://goal-int.org/rol-analitichnoi-diyalnosti-ta-analitichnix-centriv-u-formuvanni-j-realizacii-kiberbezpekovoi-politiki/

21. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* 2021. № 9. С. 332-334. URL: http://www.lsej.org.ua/9_2021/85.pdf

22. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв'язку*. 2016. Вип. 4. С. 81–84. URL: http://nbuv.gov.ua/UJRN/suntz2016422

23. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ, 2013. 476 с.

24. Пашнєв Д.В. Стратегія забезпечення кримінологічної кібернетичної безпеки органами внутрішніх справ. *Вісник Кримінологічної асоціації України*. 2014. № 8. URL: http://files.visnikkau.org/200000574-2ccb52dc47/Visnyk8_10.pdf

25. Пащенко Т. П. Гібридна війна та соціальні мережі. *Інформаційний вимір гібридної війни*: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62–65

26. Пащенко Т. П. Гібридна війна та соціальні мережі. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62-65

27. Присяжнюк М. М., Бєлошевич Я. С. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 37–41

28. Прощаєв В.В. Принципи розвідувальної діяльності за законодавством країн пострадянського простору: порівняльний аналіз. Науковий вісник публічного та приватного права. Випуск 1, том 1, 2019. С. 96-10

29. Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE). *Україна в системі глобального інформаційного обміну*: теоретико-методологічні аспекти дослідження і підготовки фахівців : всеукраїнська наукова конференція, Львів, 27 травня 2011 р. / Національний університет "Львівська політехніка". – Львів : Видавництво Львівської політехніки, 2011. – С. 257–261 URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content

30. Розвідка на основі відкритих джерел. URL: https://sidcon.com.ua/ru/osint

31. Розвідувальний процес за поглядами воєнних фахівців НАТО. URL: https://bintel.org. ua/nukma/rozviduvalnij-proces-nato

32. Савінова Н.А. Кібернетична інтервенція: до питань походження та потреби криміналізації в умовах формування та розвитку інформаційного суспільства. URL: http://justinian.ua/article.php?id=3912

33. Серватнюк М. Інтеграція методів OSINT в систему управління інформаційним ризиками. ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ : IX науково-техн. конф., м. Тернопіль, 8–9 груд. 2021 р. 2021. с. 76

34. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз: монографія / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браіловський. Київ: Формат, 2021. 407 с.

35. Страдний І.О. Протидія кіберзлочинам у сфері використання платіжних систем. *Кібербезпека у системі національної безпеки України*: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу,

м. Маріуполь, 26 квітня 2018 р. / Маріупольський державний університет; уклад. Проценко О.Б., Меркулова К.В. Маріуполь: МДУ, 2018. 145 с. С. 34-36. URL: http://mdu.in.ua/Nauch/Konf/2018/kiberbezpeka_24_04.pdf

36. Ткачук Н. Кібертероризм як новий виклик національній безпеці. *Протидія терористичній діяльності*: міжнародний досвід і його актуальність для України : матеріали Міжнар. наук.-практ. конф. (30 вересня 2016 року). Київ : Національна академія прокуратури України, 2016. С. 340–342

37. Федорчук С. Цілі і завдання інтернет-розвідки. *Природничі та гуманітарні науки. Актуальні питання*: матеріали IX Всеукраїнської студентської науково-технічної конференції, 20-21 квітня 2016 року - Т. : ТНТУ, 2016. Том 1. С. 116-117

38. Цаль-Цалко Ю.С., Мороз Ю.Ю. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства*: збірник наукових праць, том IV, частина І, Житомир: ПП «Рута», 2017 С. 8-11

39. Цимбалюк В.С. Основи інформаційного права України: [навч. посібн.] / [В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К.: Знання, 2004. 274 с.

40. Череповський К.П. Інкорпорація інформаційного законодавства України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» . Запоріжжя, 2013. 19 с.

41. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342-348. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2010_23_41.pdf

42. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-

Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

Ресурси відкритого доступу

1. Каталог правових сайтів України - http://pravoved.in.ua
2. Єдиний веб-портал послуг - http://www.kmu.gov.ua
3. Національне антикорупційне бюро України - https://nabu.gov.ua
4. Офіс генерального прокурора - http://www.gp.gov.ua
5. Служба безпеки України - http://www.sbu.gov.ua
6. Міністерство внутрішніх справ - http://www.mvs.gov.ua
7. Департамент кіберполіції Національної поліції України - https://cyberpolice.gov.ua
8. Державна служба спеціального зв'язку та захисту інформації України - https://cip.gov.ua/ua
9. Державний центр кіберзахисту та протидії кіберзагрозам - https://scpc.gov.ua/uk
10. Антирейдерський союз підприємців України - http://antiraider.ua
11. Центр протидії корупції - http://antac.org.ua
12. Державний земельний кадастр - https://e.land.gov.ua/auth_select
13. Система закупівель ProZorro - https://prozorro.gov.ua/uk
14. Фонд державного майна. Кабінет користувача єдиної бази данних звітів про оцінку - https://evaluation.spfu.gov.ua/
15. Єдиний державний реєстр судових рішень - https://reyestr.court.gov.ua/
16. Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань - https://usr.minjust.gov.ua/content/free-search
17. Державний реєстр речових прав на нерухоме майно - https://online.minjust.gov.ua/rrp/

18. Єдиний державний реєстр декларацій - https://public.nazk.gov.ua/

19. Автоматизована система виконавчого провадження - https://asvpweb.minjust.gov.ua/#/search-debtors

20. Єдиний державний реєстр осіб, які вчинили корупційні або пов’язані з корупцією правопорушення - https://corruptinfo.nazk.gov.ua/

НАВЧАЛЬНЕ ВИДАННЯ

OSINT

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для підготовки до практичних занять та самостійної роботи
здобувачів першого (бакалаврського) рівня вищої освіти
в галузі знань 12 «Інформаційні технології»

Електронне видання

Укладачі:

Аркуша Лариса Ігорівна

Дикий Олег Вікторович

Мандриченко Жанна Василівна

Стоянов Микола Михайлович

Сидорчук Владислав Васильович

В авторській редакції