МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Методичні рекомендації для підготовки до практичних занять

(для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності D8 «Право»)

Дніпро
2026

УДК 004.9+34.096
С 38

Схвалено Науково-методичною радою
Дніпровського державного
університету внутрішніх справ
(протокол № 6 від 18.02.2025)

РЕЦЕНЗЕНТИ:

доктор юридичних наук, доцент **Олексій ТИТАРЕНКО** – начальник науково-дослідної лабораторії з підготовки військ Київського інституту Національної гвардії України;
кандидат технічних наук, доцент **Ольга СТАНІНА** – доцент кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка».

С 38 Синиціна Ю. П. Сучасні інформаційні технології в юридичній діяльності: метод. рекомендації для підгот. до практ. занять (для здобувачів другого (магістерського) рівня вищ. освіти зі спец. D8 «Право»). Дніпро : Дніпров. держ. ун-т внутр. справ, 2026. 55 с.

Методичні рекомендації розроблені для підготовки до практичних занять із тем, що передбачені навчальним планом із дисципліни «Сучасні інформаційні технології в юридичній діяльності». Містять основні теоретичні положення, завдання, вимоги до оформлення та приклади виконання практичних робіт, запитання для підсумкового контролю, словник термінів і список літератури.

Для здобувачів другого рівня вищої освіти зі спеціальності D8 «Право» заочної форми навчання та викладачів закладів вищої освіти.

УКЛАДАЧ:

кандидат технічних наук, доцент **Юлія СИНИЦІНА** – доцент кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ.

ЗМІСТ

Вступ …… 4

ТЕМА 1. Використання штучного
інтелекту в правозастосовній практиці:
можливості, ризики та етичні виклики …… 7

ТЕМА 2. Цифрова доказова база у кримінальному
та цивільному процесах: збір, збереження та
допустимість…… 10

ТЕМА 3. Кібербезпека юридичних даних:
методи та стратегії інформаційної безпеки …….. 14

ТЕМА 4. Пошук правової інформації
в мережі інтернет. особиста безпека
в інтернеті ……..…... 19

Запитання для підсумкового контролю
з навчальної дисципліни «Сучасні інформаційні технології
в юридичній діяльності» ……..…….. 29

Список основної літератури до навчальної дисципліни
«Сучасні інформаційні технології в юридичній діяльності» ……. 31

Система оцінювання успішності з навчальної дисципліни
«Сучасні інформаційні технології в юридичній діяльності» ……. 36

Словник термінів ……..……..……... 41

Додаток 1 ……..……..……..…….. 44

Додаток 2 ……..……..……..…….. 46

Додаток 3 ……..……..……..….. 49

Додаток 4 ……..……..……..…….. 51

Додаток 5 ……..……..……..…….. 52

ВСТУП

У сучасній юридичній науці та практиці дедалі більшої ваги набуває тема використання сучасних інформаційних технологій, здатних ефективно відображати складність правових процесів та управлінських рішень. Цифрові інструменти – це потужний засіб для автоматизації аналітичної роботи, обробки великих масивів правової інформації, виявлення закономірностей у судовій практиці, моделювання правових ситуацій та прийняття обґрунтованих рішень. Використання інформаційних технологій підвищує точність, оперативність і прозорість правозастосовної діяльності, що є особливо важливим для підготовки фахівців-правників магістерського рівня.

Метою вивчення навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності» є підготовка висококваліфікованих фахівців, здатних виконувати складні спеціалізовані завдання і практичні проблеми в юридичній діяльності, зокрема за допомогою навичок практичної роботи з сучасними інформаційними системами та технологіями.

Очікувані результати навчання:

знати:

– основні поняття та апаратно-програмне забезпечення інформаційних технологій;

– особливості застосування штучного інтелекту в правозастосовній практиці: можливості, ризики та етичні виклики;

– основи кібербезпеки юридичних даних: методи та стратегії інформаційної безпеки;

– теоретичні поняття та можливості інформаційних технологій, комп’ютерних мереж;

– основні можливості інформаційно-пошукових систем у сфері законодавства;

– особливості комплексного використання прикладного програмного забезпечення в юридичній діяльності.

вміти:

– застосовувати методи та стратегії інформаційної безпеки у професійній діяльності;

– здійснювати аналіз цифрових доказів у кримінальному та цивільному процесах: збір, збереження та допустимість;

– здійснювати пошук необхідної інформації у сфері юридичної діяльності з використанням можливостей веббраузерів, критично та системно аналізувати знайдену інформацію;

– працювати в режимі користувача з основними інформаційно-пошуковими системами у сфері законодавства, здійснювати пошук та аналіз новітньої інформації у сфері юридичної діяльності;

– застосовувати спеціальні інформаційні технології для захисту інформації у професійній діяльності;

– комплексно використовувати прикладне програмне забезпечення для повного та всебічного встановлення необхідних обставин у сфері юридичної діяльності.

Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою: Право.

Інтегральна компетентність – здатність виконувати завдання дослідницького та/або інноваційного характеру у сфері права.

Загальні компетентності:

ЗК1 – здатність до абстрактного мислення, аналізу та синтезу.

ЗК2 – здатність проводити дослідження на відповідному рівні.

ЗК3 – здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК4 – здатність до адаптації та дії в новій ситуації.

ЗК6 – здатність генерувати нові ідеї (креативність).

ЗК7 – здатність приймати обґрунтовані рішення.

ЗК10 – здатність розробляти проєкти та управляти ними.

Спеціальні компетентності:

СК10 – здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування.

СК13 – здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень із належною аргументацією.

СК14 – здатність самостійно готувати проєкти нормативно-правових актів, обґрунтовувати суспільну обумовленість їх прийняття, прогнозувати результати їхнього впливу на відповідні суспільні відносини.

СК15 – здатність самостійно готувати проєкти актів правозастосування, зважаючи на вимоги щодо їхньої законності, обґрунтованості та вмотивованості.

Пререквізити та постреквізити дисципліни:

Пререквізити: «Інформаційні технології».

Постреквізити: Кваліфікаційна робота.

Здобувачі вищої освіти повинні продемонструвати такі **результати навчання**:

РН3 – проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включно з науковою та професійною літературою, базами даних, цифровими, статистичними, тестовими та ін., та перевіряти їх на достовірність, використовуючи сучасні методи дослідження.

РН8 – оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

РН9 – генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.

РН17 – інтегрувати необхідні знання та виконувати складні завдання зі правозастосування у різних сферах професійної діяльності.

Видання містить методичні рекомендації для підготовки до практичних занять за темами навчальної дисципліни, запитання для підсумкового контролю, словник термінів, а також список літератури.

ТЕМА 1. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВОЗАСТОСОВНІЙ ПРАКТИЦІ: МОЖЛИВОСТІ, РИЗИКИ ТА ЕТИЧНІ ВИКЛИКИ

Зміст теми:

Поняття та основні напрями застосування штучного інтелекту (далі – AI) у праві. Інструменти AI для автоматизації юридичних досліджень (CaseLaw, ROSS, ChatGPT тощо). Використання AI для прогнозування судових рішень: приклади та обмеження. Юридичні ризики: конфіденційність, упередженість алгоритмів, правовий статус AI-рішень. Етичні стандарти та рекомендації міжнародних організацій.

Практичне заняття № 1 – 2 год.

Мета: ознайомити здобувачів освіти із сучасними AI-інструментами для правового пошуку, протестувати їхню ефективність та порівняти з традиційними базами даних.

План:

1. Робота з онлайн-сервісами правового пошуку;
2. Порівняння результатів з традиційним пошуком у базах даних;
3. Обговорення виявлених переваг і недоліків.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *штучний інтелект, машинне навчання, правозастосування, алгоритмізація, автоматизований правовий аналіз, етичні виклики, правова відповідальність AI, прогнозування судових рішень, кібербезпека, правова експертиза з AI.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Аналіз сучасних інструментів AI для обробки правової інформації.

Сучасні інструменти штучного інтелекту активно інтегруються в юридичну діяльність. Вони здатні виконувати правовий пошук, аналізувати великі масиви судової практики та нормативних актів, створювати аналітичні звіти. Найпоширенішими є ChatGPT, CaseText, ROSS Intelligence, Harvey AI, які допомагають юристам швидко отримувати релевантну інформацію, формувати проєкти процесуальних документів, проводити порівняльний аналіз норм. Їхня перевага полягає у високій швидкості пошуку та можливості працювати з великими обсягами даних. Водночас залишається потреба у перевірці результатів, адже системи можуть помилятися або надавати неповні покликання на джерела.

2. *Автоматизація юридичних досліджень і прогнозування судових рішень*.

AI-системи використовуються для автоматизації юридичних досліджень: від пошуку прецедентів і правових норм до підготовки довідок і проєктів договорів. Алгоритми аналізують великі бази рішень, виявляють закономірності та пропонують релевантні матеріали за заданим запитом. Особливо перспективним напрямом є прогнозування судових рішень, коли AI моделює ймовірність певного результату на основі попередньої практики. Такі інструменти допомагають адвокатам будувати стратегію захисту, оцінювати ризики та прогнозувати перспективу справи. Водночас вони не можуть гарантувати точність у 100 %, адже враховують лише формальні дані без урахування людського фактора (позиції судді, процесуальної тактики).

3. Регуляторні та етичні обмеження.

Використання AI у правозастосуванні пов'язане з низкою регуляторних і етичних викликів. Основними з-поміж них є:

– *конфіденційність* – захист персональних і чутливих юридичних даних від несанкціонованого доступу;

– *прозорість алгоритмів* – необхідність розуміння логіки рішень AI, щоб уникати прихованої упередженості;

– *відповідальність* – проблема визначення, хто несе юридичну відповідальність за помилку AI: розробник, користувач чи організація;

– *етичність* – заборона дискримінації та упереджених висновків на основі алгоритмічних рішень.

Європейський Союз, США та інші країни вже розробляють правові межі для використання AI, зокрема щодо захисту даних (General Data Protection Regulation, GDPR), недопущення зловживань і встановлення стандартів безпеки. Для України актуальним питанням є гармонізація законодавства з міжнародними підходами та створення власних етичних стандартів.

Завдання:

Завдання № 1. Зареєструватися у двох сервісах на вибір здобувача (наприклад, ChatGPT та Gemini). Приклад виконання – додаток 1.

Завдання № 2. Виконати правовий пошук за власним запитом. Приклад: «Порядок розірвання договору оренди в Україні».

Завдання № 3. Порівняти точність і повноту результатів.

Завдання № 4. Заповнити таблицю порівняння (швидкість, зручність, глибина пошуку).

Завдання № 5. Пройти тест за темою практичної роботи.

Вимоги до оформлення практичної роботи

Тема: Огляд та тестування AI-сервісів для юристів.

Мета: ознайомитися з сучасними AI-інструментами для правового

пошуку, протестувати їхню ефективність та порівняти з традиційними базами даних.

1. Загальні вимоги.

Робота виконується у текстовому редакторі MS Word/Google Docs в електронному вигляді (формати .docx, для використання у системах СУДН «Moodle»).

Обсяг – 8–12 сторінок друкованого тексту.

Формат сторінки: А4; поля: верхнє – 20 мм, нижнє – 20 мм, ліве – 25 мм, праве – 15 мм. Шрифт: Times New Roman, розмір – 14 пт.

Інтервал – 1,5. Абзацний відступ – 1,25 см. Нумерація сторінок – з правого нижнього кута.

Усі таблиці, рисунки, схеми повинні мати назву та номер.

Використані джерела подаються у списку літератури оформленими за ДСТУ 8302:2015 (оформлення бібліографічних посилань).

2. Структура роботи.

Титульний аркуш (назва міністерства, назва закладу, дисципліна, тема, дані здобувача вищої освіти і викладача, рік).

Мета та завдання роботи.

Хід виконання роботи:

Крок 1. Вибір інструментів (з поясненням).

Крок 2. Формування правового запиту.

Крок 3. Робота з AI-сервісами (результати кожного інструменту).

Крок 4. Робота з традиційною базою даних (аналіз ЄДРСР).

Крок 5. Порівняльний аналіз (таблиця + коментарі).

Висновки (3–5 узагальнених тез про результати роботи).

Список використаних джерел (не менше 5, у тому числі нормативні акти).

Додатки (за наявності: скриншоти роботи з сервісами, фрагменти результатів пошуку).

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Надайте визначення штучного інтелекту та назвіть основні напрями його застосування у праві.
2. Які AI-інструменти використовуються для автоматизації юридичних досліджень?
3. У чому полягає принцип роботи системи прогнозування судових рішень?
4. Які фактори можуть впливати на точність прогнозів AI у судових справах?
5. Назвіть приклади міжнародних ініціатив зі стандартизації етичного використання AI у праві.
6. Які основні юридичні ризики пов’язані з використанням AI у правозастосуванні?

7. Що таке алгоритмічна упередженість та як вона може впливати на судові рішення?

8. Як AI може підвищити ефективність роботи адвокатів та юристів?

9. Чим відрізняється правовий статус рішень, ухвалених AI, від рішень людини?

10. Які етичні виклики постають при впровадженні AI у правову сферу?

ТЕМА 2. ЦИФРОВА ДОКАЗОВА БАЗА У КРИМІНАЛЬНОМУ ТА ЦИВІЛЬНОМУ ПРОЦЕСАХ: ЗБІР, ЗБЕРЕЖЕННЯ ТА ДОПУСТИМІСТЬ

Зміст теми:

Поняття та класифікація електронних доказів. Правові вимоги до збору та подання цифрових доказів. Методи фіксації та збереження електронної інформації. Цифрова криміналістика: інструменти та технічні процедури. Судова практика України та міжнародні підходи.

Практичне заняття № 2 – 2 год.

Мета: ознайомити здобувачів освіти з особливостями використання електронних доказів у судовій практиці. Сформувати практичні навички аналізу реальних кейсів, оцінки їх доказової сили та процесуального значення. Розвинути вміння ідентифікувати, перевіряти та інтерпретувати електронні докази в межах правозастосовної діяльності.

План:

1. Визначення допустимості доказів;
2. Виявлення помилок при зборі або поданні;
3. Обговорення можливих стратегій захисту.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *електронний доказ, метадані, електронний документ, кваліфікований електронний підпис (КЕП), цифровий слід, допустимість доказу, автентичність доказу, ланцюг збереження, електронне листування, цифрова криміналістика.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Поняття та класифікація електронних доказів.

Електронні докази – це будь-яка інформація, створена, збережена або передана в цифровій формі, яка може підтверджувати чи спростовувати факти,

що мають значення для судового процесу. Електронні докази охоплюють електронні документи, цифрові зображення, відео, електронне листування, дані з соціальних мереж, записи телефонних розмов, лог-файли комп'ютерних систем, метадані тощо.

Класифікація електронних доказів:

– електронні документи (контракти, заяви, рахунки з кваліфікованим електронним підписом (далі – КЕП));

– електронна комунікація (електронні листи, листування в месенджерах);

– мультимедійні файли (у фото-, відео-, аудіоформатах);

– технічні дані (лог-файли серверів, дані GPS, IP-адреси);

– інтернет-контент (сторінки сайтів, публікації у соціальних мережах).

2. Правові вимоги до збору та подання цифрових доказів.

Законодавство України та міжнародні стандарти вимагають, щоб електронні докази відповідали принципам *належності, допустимості та достовірності*.

Основні вимоги:

– *законність отримання* – доказ має бути зібраний уповноваженими особами або у встановленому законом порядку;

– *цілісність* – дані не повинні зазнавати змін після збору; підтверджується контрольними хеш-сумами та протоколами;

– *автентичність* – доказ повинен походити від заявленого джерела, підтверджуватися КЕП, метаданими чи експертизою;

– *процесуальна форма* – докази подаються до суду у вигляді електронних документів із накладеним КЕП або у вигляді копій із електронних носіїв із засвідченням їхньої автентичності.

3. Методи фіксації та збереження електронної інформації.

Щоб електронні докази були прийняті судом, необхідно забезпечити правильну фіксацію та збереження:

– *створення цифрових копій* за допомогою спеціальних інструментів (наприклад, EnCase, FTK);

– *використання хеш-функцій* (MD5, SHA-256) для підтвердження незмінності даних;

– *протоколювання дій* – ведення документації всіх етапів збору й зберігання (chain of custody);

– *використання скриншотів та відеозаписів* при фіксації вебсторінок чи листування;

– *зберігання у захищених сховищах* із обмеженим доступом та шифруванням.

4. Методи та інструменти OSINT-технологій.

OSINT (Open Source Intelligence) – це збір та аналіз інформації з відкритих джерел для отримання розвідувальних даних, які можуть мати доказове значення у суді.

Основні методи OSINT:

– пошук даних у відкритих базах (реєстри, кадастри, судові рішення);
– моніторинг соціальних мереж та месенджерів;
– аналіз вебсайтів та форумів;
– геолокація та аналіз зображень через метадані;
– використання пошукових операторів у Google (Google Dorking).

Інструменти OSINT.

Maltego – для аналізу зв'язків між об'єктами.

Shodan – пошук пристроїв та серверів в інтернеті.

TheHarvester – збір e-mail та доменної інформації.

Social Links, SpiderFoot – комплексний аналіз соціальних мереж і цифрових слідів.

Wayback Machine – архівування вебсторінок.

Завдання:

Завдання № 1. Ознайомитися з одним із рішень судів України, де використовувалися електронні докази або вибрати для виконання один із запропонованих кейсів (додаток 2). Приклад виконання – додаток 3.

Завдання № 2. Визначити, чи були ці докази визнані допустимими.

Завдання № 3. Підготувати аргументи «за» і «проти» визнання доказу.

Завдання № 4. Пройти тест за темою.

Вимоги до оформлення кейсів

1. Загальні положення.

Кейс має бути оформлений у письмовій формі (електронний варіант).

Обсяг: 3–5 сторінок (без додатків).

Мова викладу: українська, науково-офіційний стиль.

Структурованість: чіткий поділ на логічні частини з підзаголовками.

2. Структура кейсу.

Назва кейсу – коротка, відображає сутність проблеми (до 15 слів).

Вступ (ситуаційний контекст) – опис умов, у яких виникла проблема (час, місце, учасники, вихідні дані).

Проблема/завдання – чітке формулювання питання чи виклику, що потребує вирішення.

Основна інформація (факти) – дані, на основі яких студенти повинні зробити висновки (статистика, документи, витяги із законодавства, опис дій).

Запитання для аналізу/завдання – не менше 3–5 відкритих запитань, що спонукають до обговорення та пошуку рішень.

Орієнтовні напрями вирішення – можливі варіанти відповідей (коротко, для викладача).

Очікувані результати навчання – які знання, уміння чи компетентності мають бути сформовані після роботи з кейсом.

3. Вимоги до змісту.

Актуальність проблеми для правоохоронної діяльності.

Використання AI/ML-технологій як інструменту аналізу чи вирішення проблеми.

Обов'язкове врахування правових та етичних аспектів (захист персональних даних, права людини).

Можливість різних підходів до розв'язання (немає єдиної правильної відповіді).

Орієнтація на розвиток у здобувачів аналітичного та критичного мислення.

4. Оформлення.

Шрифт: Times New Roman, 14 пт.

Інтервал: 1,5.

Поля: 2,0 см з усіх боків.

Нумерація сторінок – у правому нижньому куті.

Використання таблиць, схем, ілюстрацій – за потреби (з підписами).

Посилання на джерела – згідно з ДСТУ 8302:2015 (оформлення бібліографічних посилань).

5. Форма представлення.

У друкованому вигляді (для аудиторної роботи).

В електронному вигляді (формати .docx, .pdf, .pptx – для використання у системах СУДН «Moodle»).

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Надайте визначення електронних доказів та їхніх основних видів.
2. Якими є вимоги законодавства України до збору електронних доказів?
3. Як забезпечується автентичність електронних доказів у суді?
4. Що таке цифровий ланцюг збереження доказів (chain of custody)?
5. Які методи фіксації електронної інформації застосовуються у криміналістиці?
6. Як відрізняється допустимість електронних доказів у кримінальному та цивільному процесах?
7. Назвіть приклади міжнародних стандартів роботи з електронними доказами.
8. У чому полягає роль експерта з цифрової криміналістики у судовому процесі?
9. Які інструменти використовуються для відновлення видаленої цифрової інформації?
10. Які типові помилки призводять до визнання електронних доказів недопустимими?

ТЕМА 3. КІБЕРБЕЗПЕКА ЮРИДИЧНИХ ДАНИХ: МЕТОДИ ТА СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Зміст теми:

Огляд сучасних викликів і загроз інформаційній безпеці в юридичній діяльності. Стратегії захисту конфіденційної інформації від зовнішніх загроз. Аналіз інноваційних технологій та інструментів для захисту інформації. Методи технічного захисту інформації. Організаційні заходи: політики доступу, аудит безпеки. Захист персональних даних.

Практичне заняття № 3 – 2 год.

Мета: ознайомити здобувачів освіти з правовими та технічними основами захисту персональних даних. Навчити визначати ризики та застосовувати сучасні інформаційні технології для їх мінімізації.

План:

1. Ознайомлення з основними правовими вимогами у сфері захисту персональних даних;
2. Здійснення аналізу ризиків обробки персональних даних у цифровому середовищі;
3. Засвоєння практичних інструментів забезпечення безпеки персональної інформації (шифрування, багатофакторна автентифікація, контроль доступу);
4. Розвинення навичок застосування законодавчих норм (Закон України «Про захист персональних даних», GDPR) у професійній юридичній діяльності.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *персональні дані, суб'єкт персональних даних, володілець персональних даних, розпорядник персональних даних, обробка персональних даних, чутливі персональні дані, згода на обробку персональних даних, захист персональних даних, конфіденційність, право на забуття.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Персональні дані.

Персональні дані – це будь-яка інформація, що дає змогу прямо або опосередковано ідентифікувати фізичну особу. До них належать: прізвище, ім'я та по батькові, дата і місце народження, адреса проживання, номер

телефону, адреса електронної пошти, ідентифікаційний код, дані паспорта, фотографії, відомості про місце роботи, освіту тощо.

Особливу категорію становлять чутливі персональні дані, що вимагають підвищеного рівня захисту. Це, зокрема, інформація про стан здоров'я, біометричні та генетичні дані, релігійні чи політичні переконання, дані про судимість.

Вітчизняне законодавство (Закон України «Про захист персональних даних») передбачає, що обробка персональних даних може здійснюватися лише з метою, визначеною володільцем бази даних, і за умови отримання згоди суб'єкта персональних даних, крім випадків, прямо передбачених законом.

Обробка персональних даних охоплює їх збирання, реєстрацію, накопичення, зберігання, використання, поширення, знеособлення та знищення. При цьому важливо забезпечувати принципи законності, пропорційності та безпеки обробки.

Захист персональних даних передбачає застосування організаційних і технічних заходів, які запобігають несанкціонованому доступу, зміні чи знищенню інформації. З-поміж таких заходів – шифрування, багатофакторна автентифікація, контроль доступу, резервне копіювання, політика конфіденційності.

Права суб'єктів персональних даних:

– право знати, які саме дані обробляються;
– право доступу до своїх даних;
– право вимагати виправлення чи видалення даних;
– право на забуття, передбачене європейським законодавством (GDPR).

Таким чином, персональні дані є важливим об'єктом правового захисту у цифрову добу. Їх належне збереження та використання є гарантією поваги до приватного життя людини та запобігання зловживанням.

2. Основні принципи захисту персональних даних.

Захист персональних даних ґрунтується на міжнародних стандартах (зокрема, GDPR у ЄС) та законодавстві України (Закон України «Про захист персональних даних»). Метою є гарантування права людини на приватність і недоторканність особистого життя.

2.1. Законність і справедливість.

Персональні дані повинні оброблятися лише на законних підставах: за згодою особи або у випадках, передбачених законом. Обробка має здійснюватися прозоро та чесно щодо суб'єкта даних.

2.2. Цільове призначення.

Дані можуть збиратися та використовуватися тільки з визначеною і чіткою метою. Використання їх у інших цілях є порушенням прав людини.

2.3. Мінімізація даних.

Необхідно збирати лише ті дані, які є дійсно потрібними для досягнення мети обробки. Надлишкове або зайве збирання інформації заборонене.

2.4. Точність і актуальність.

Персональні дані повинні бути точними, повними та оновлюватися у разі потреби. Використання застарілих або недостовірних даних може завдати шкоди особі.

2.5. Обмеження строків зберігання.

Дані зберігаються лише протягом часу, необхідного для досягнення мети їх обробки. Після цього вони повинні бути видалені або знеособлені.

2.6. Конфіденційність і безпека.

Володілець бази даних зобов'язаний забезпечити належні технічні та організаційні заходи для захисту від несанкціонованого доступу, втрати чи знищення даних.

2.7. Відповідальність (принцип підзвітності).

Особи та організації, які обробляють персональні дані, несуть відповідальність за дотримання вимог закону. Вони повинні бути готовими довести законність і безпечність обробки даних.

3. Основні ризики у сфері захисту персональних даних.

Сучасне інформаційне суспільство створює значні виклики для безпеки персональних даних. Недотримання правил захисту може призвести до витоку конфіденційної інформації, шахрайства чи порушення прав людини. З-поміж найпоширеніших ризиків можна виділити такі:

1) витік даних. Виникає у разі несанкціонованого оприлюднення або втрати персональних даних через злам інформаційних систем, халатність працівників або недостатній рівень кіберзахисту. Це може призвести до розголошення паспортних даних, фінансової інформації чи медичних записів;

2) несанкціонований доступ – отримання доступу до персональних даних сторонніми особами без дозволу суб'єкта або власника бази даних. Часто пов'язаний із відсутністю належних паролів, багатофакторної автентифікації або контролю доступу;

3) фішинг. Цей метод шахрайства полягає в тому, що зловмисники за допомогою електронних листів, підроблених сайтів або повідомлень намагаються змусити людину розкрити свої паролі, банківські реквізити чи іншу конфіденційну інформацію;

4) соціальна інженерія – маніпулювання людьми з метою отримання доступу до інформації. Наприклад, зловмисник може представитися співробітником компанії чи державного органу, щоб змусити людину добровільно надати потрібні дані;

5) неналежне зберігання даних. Ризик виникає, коли персональні дані зберігаються без належного захисту: у відкритих базах, незашифрованих файлах чи на носіях без фізичної охорони. Це значно підвищує ймовірність їх втрати або крадіжки.

Розуміння цих ризиків дозволяє своєчасно впроваджувати ефективні заходи безпеки: використання шифрування, багатофакторної автентифікації, регулярне оновлення систем та навчання користувачів.

Практичні інструменти захисту: шифрування даних, електронний цифровий підпис, VPN, використання захищених паролів, аудит доступу.

Законодавче регулювання: Закон України «Про захист персональних даних», Загальний регламент ЄС із захисту даних (GDPR).

Завдання:

Завдання № 1. Ознайомитися з текстом Закону України «Про захист персональних даних». Приклад виконання – додаток 4.

Завдання № 2. Визначити, які персональні дані обробляються у Вашій навчальній/робочій діяльності.

Завдання № 3. Скласти таблицю ризиків (5 основних ризиків) щодо обробки персональних даних (приклад: ризик витоку даних через слабкі паролі → спосіб мінімізації: впровадження двофакторної автентифікації). Класифікацію ризиків та заходів мінімізації наведено у таблиці 1 (додаток 4).

Таблиця 1

Потенційні ризики та заходи їх мінімізації

№	Потенційний ризик	Приклад ситуації	Наслідки	Заходи мінімізації
1				
2				
3				
4				
5				

Завдання № 4. Розробити зразок письмової згоди на обробку персональних даних для умовної юридичної практики (наприклад, клієнта адвоката чи користувача онлайн-сервісу).

Завдання № 5. Виконати пошук в інтернеті та навести два приклади витоків персональних даних в Україні/світі, коротко описати їхні наслідки.

Завдання № 6. Підготувати короткі рекомендації щодо безпечної роботи з персональними даними у діяльності юриста.

Завдання № 7. Пройти тест за темою.

Вимоги до оформлення практичної роботи

Тема: Кібербезпека юридичних даних: методи та стратегії інформаційної безпеки.

1. Загальні вимоги.

Робота виконується у текстовому редакторі MS Word/Google Docs в

електронному вигляді (формати .docx, для використання у системах СУДН «Moodle»).

Обсяг – до 10 сторінок друкованого тексту.

Формат сторінки: А4, поля: верхнє – 20 мм, нижнє – 20 мм, ліве – 25 мм, праве – 15 мм.

Шрифт: Times New Roman, розмір – 14 пт.

Інтервал – 1,5. Абзацний відступ – 1,25 см.

Нумерація сторінок – з правого нижнього кута.

Усі таблиці, рисунки, схеми повинні мати назву та номер.

Використані джерела подаються у списку літератури оформленими за ДСТУ 8302:2015 (оформлення бібліографічних посилань).

2. Структура роботи.

Титульний аркуш (назва міністерства, назва закладу, дисципліна, тема, дані здобувача вищої освіти і викладача, рік).

Мета та завдання роботи.

Виконання:

Таблиця ризиків та заходів захисту.

Приклад форми згоди.

Рекомендації для юридичної фірми.

Висновки (3–5 узагальнених тез про результати роботи).

Список використаних джерел (не менше 5, у тому числі нормативні акти).

Додатки (за наявності: скриншоти роботи з сервісами, фрагменти результатів пошуку).

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке персональні дані?
2. Які основні принципи захисту персональних даних?
3. Чим відрізняється «звичайні персональні дані» від «чутливих персональних даних»?
4. Які методи технічного захисту Ви знаєте?
5. Якими є наслідки порушення законодавства у сфері захисту персональних даних?
6. Що таке GDPR та чому цей документ важливий для України?
7. Що таке витік персональних даних і які його основні причини?
8. Які категорії інформації вважаються конфіденційними в організаціях?
9. Які організаційні заходи можна застосувати для запобігання несанкціонованому доступу до даних?
10. Що таке інцидент інформаційної безпеки і як його слід документувати?

ТЕМА 4. ПОШУК ПРАВОВОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА В ІНТЕРНЕТІ

Зміст теми:

Історія розвитку та загальна характеристика пошукових систем. Пошук інформації за допомогою Google: сервіси, спеціальний пошук, апаратне забезпечення та інструменти. Метапошукові системи та системи анонімного пошуку інформації. Пошук оперативної інформації в соціальних мережах (Facebook). Застосування чат-ботів у месенджері Telegram. Особиста безпека в інтернеті.

Практичне заняття № 4 – 2 год.

Мета: ознайомити здобувачів освіти з історією розвитку пошукових систем. Навчити використовувати базові та розширені можливості Google для пошуку інформації. Опрацювати навички роботи з метапошуковими системами та системами анонімного пошуку. Розвинути практичні вміння перевірки достовірності та релевантності знайденої інформації.

План:

1. Історія розвитку та загальна характеристика пошукових систем;
2. Пошук інформації за допомогою Google: сервіси, спеціальний пошук, апаратне забезпечення та інструменти;
3. Метапошукові системи та системи анонімного пошуку інформації;
4. Базові поняття та методи соціальної інженерії: фішингові електронні листи, сайти та заражене програмне забезпечення;
5. Безпека в інтернеті: онлайн-репутація, шкідливий онлайн-контент, секстинг, сексторшен, кіберсталкінг;
6. Безпека в інтернеті: кібербулінг, кібергрумінг, тролінг, флеймінг, хепіслепінг, хейтспіч, доксинг, кетфішинг.

Основні поняття, терміни та категорії, що підлягають засвоєнню: *OSINT (Open Source Intelligence), метапошукова система, соціальна інженерія, цифровий слід, пошукові системи, анонімізація, спеціалізований пошук, фішинг, кібергігієна, достовірність джерела.*

ОСНОВНІ ТЕОРЕТИЧНІ ПОЛОЖЕННЯ

1. Історія розвитку та загальна характеристика пошукових систем.

Пошукові системи виникли як відповідь на зростання обсягів інформації в мережі Інтернет. Перші пошукові каталоги з’явилися у 1990-х роках і мали

вигляд списків сайтів, які вручну додавали адміністратори (наприклад, Yahoo Directory). Згодом виникла потреба в автоматизованих системах, здатних швидко індексувати та знаходити дані.

У 1993 р. з'явився Archie, який вважають першим інструментом пошуку файлів у мережі. Пізніше виникли AltaVista, Lycos, Excite, які впровадили алгоритми індексації та пошуку за ключовими словами. Справжній прорив зробила компанія Google у 1998 р., запропонувавши алгоритм PageRank, що визначав важливість сторінки на основі кількості та якості посилань.

Сучасні пошукові системи – це складні програмно-апаратні комплекси, що використовують штучний інтелект, машинне навчання та великі бази даних для швидкого доступу до потрібної інформації. Вони дозволяють працювати з мультимедіа, картами, науковими статтями, новинами та іншими ресурсами.

2. Пошук інформації за допомогою Google: сервіси, спеціальний пошук, апаратне забезпечення та інструменти.

Google є найпопулярнішою пошуковою системою у світі. Вона надає широкий набір сервісів для різних цілей:

Google Search – основний пошук за ключовими словами та фразами;

Google Scholar – спеціалізований пошук наукових публікацій;

Google Books – пошук книг і журналів;

Google News – агрегатор новин;

Google Images – пошук зображень, включно з інструментами зворотного пошуку;

Google Maps та Google Earth – пошук географічних даних, карт і навігації;

Google Patents – пошук патентів;

Google Trends – аналіз популярності запитів.

Для роботи зі спеціальними запитами існують оператори пошуку:

«» – точна фраза;

site: – пошук на конкретному сайті;

filetype: – пошук файлів певного формату;

intitle: – пошук у заголовках сторінок.

Google використовує величезні дата-центри, потужні сервери, алгоритми штучного інтелекту та системи кешування для обробки мільярдів запитів щодня.

3. Метапошукові системи та системи анонімного пошуку інформації.

Окрім класичних пошуковиків, існують метапошукові системи, які одночасно надсилають запити до кількох пошукових систем і агрегують результати. Приклади: Dogpile, Metacrawler, Startpage. Вони дозволяють отримати більш широкий спектр результатів без обмеження одним джерелом.

Системи анонімного пошуку забезпечують конфіденційність користувача. Вони не зберігають історію пошуку та не відслідковують IP-адресу. Найвідоміші приклади:

DuckDuckGo – не відстежує користувачів і не персоналізує результати;

Startpage – використовує результати Google, але приховує дані користувача;

YaCy – децентралізована пошукова система з відкритим кодом.

Використання Tor Browser дозволяє здійснювати пошук анонімно та обходити цензуру.

Таким чином, сучасний пошук в інтернеті розвивається у двох напрямах: з одного боку – більш точні та швидкі алгоритми (Google, Bing), а з іншого – зростає попит на захист конфіденційності (DuckDuckGo, Tor).

4. Базові поняття та методи соціальної інженерії: фішингові електронні листи, сайти та заражене програмне забезпечення.

Соціальна інженерія – це наука, що вивчає людську поведінку та чинники, які на неї впливають. Для цього вона й була створена. Проте наразі активно використовується для планування та проведення кібератак. У цьому контексті соціальна інженерія – це техніки впливу та маніпулювання людьми, щоб здобути довіру або переконати їх виконати певні дії. Такий підхід ґрунтується не на технічних вразливостях, а на експлуатації людських слабкостей, як-от довірливість чи страх. Він побудований на розумінні психології людини та використанні цих знань для досягнення конкретних цілей: отримання даних для входу на сайт, вимагання грошей чи поширення особистих фотографій.

Існує декілька методів використання соціальної інженерії:

1) без прямого контакту з цільовою особою. Цей метод полягає у використанні особистої інформації для підбирання паролів (день народження, імена членів родини або номер телефону). Також злочинці можуть маніпулювати системами відновлення паролів, відповідаючи на секретні питання, як-от про дівоче прізвище матері;

2) без прямого контакту з цільовою особою, але через третіх сторін. Цей метод складається зі звернень до служб підтримки, друзів, знайомих або родичів людини, щоб отримати інформацію або вплинути на них так, щоб ті виконали певні дії, наприклад надали конфіденційну інформацію;

3) під час прямої комунікації з цільовою особою. Цей метод застосовується у тому випадку, коли шахрай вдає з себе представника служби підтримки, керівника, поліцейського або іншу особу, щоб переконати жертву надати конфіденційну інформацію або виконати дії, які можуть бути шкідливими для неї.

Методи соціальної інженерії: фішингові електронні листи, сайти та заражене програмне забезпечення.

Соціальна інженерія – це методи маніпуляцій людьми, щоб примусити

їх розголосити конфіденційну інформацію або виконати певні дії. Замість того, щоб зламувати захист IT-систем, зловмисники намагаються «зламати» самих користувачів.

Типові методи соціальної інженерії містять фішинг, видавання себе за іншу людину, шантаж, пропонування хабарів тощо. Мета одна – маніпулювати жертвою, аби отримати потрібні дані чи доступ.

Існує кілька видів застосування методів соціальної інженерії.

Фішингові електронні листи (рис. 1).

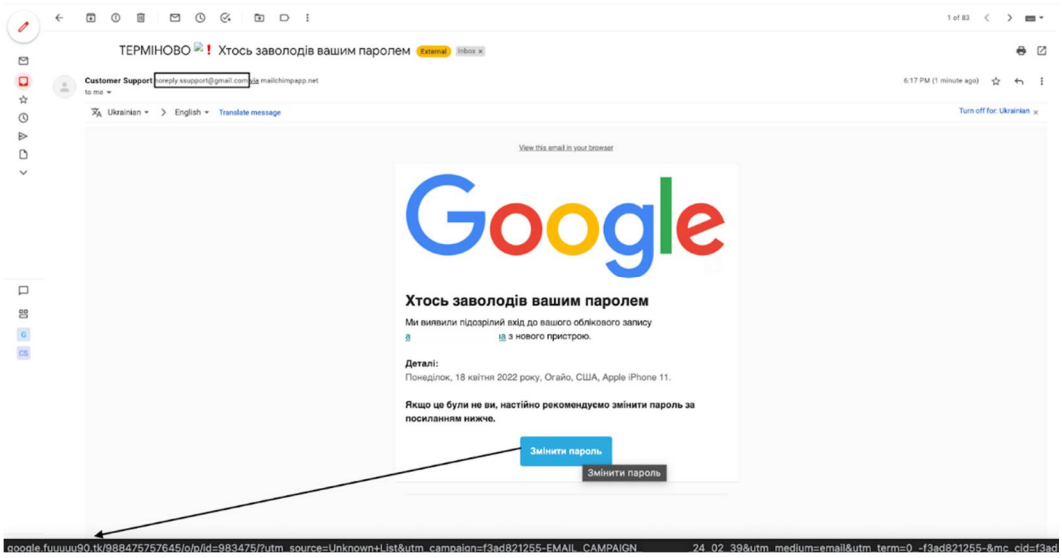

Рис. 1. Загальний вигляд фішингового електронного листа

Найчастіше такі листи потрапляють у спам, але трапляються винятки, тож слід бути вкрай обачними. На рис. 1 наведено приклад електронного листа, що спонукає змінити пароль та має всі ознаки фішингу.

Фейкові сайти.

Вони можуть мати вигляд легітимних та з'являтися в результатах пошуку. Аби переконатися, що сайт є безпечним, слід використовувати інструмент перевірки від Google (перевірити, чи є у нього сертифікат SSL (замочок) для захисту особистих даних). Варто бути обачним із сайтами з незвичним дизайном та помилками в тексті, оскільки це є ознаками того, що ресурси фейкові.

Неліцензійне програмне забезпечення (рис. 2).

Рис. 2. Загальний вигляд неліцензійного програмного забезпечення.

Це програми, що використовуються без офіційної ліцензії або правового дозволу. Так, восени 2022 р. через торент-трекери поширювали неліцензійну заражену вірусом версію Windows 10, щоб збирати дані та атакувати працівників урядових установ України.

Фішинг у месенджерах (рис. 3).

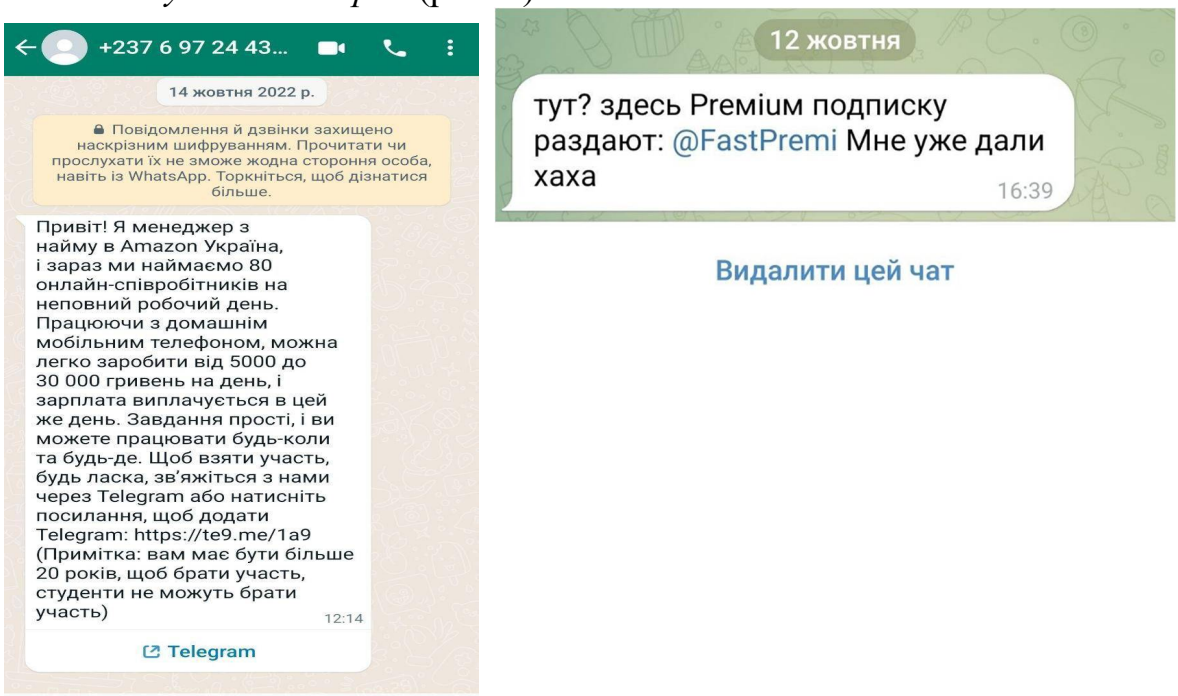

Рис. 3. Загальний вигляд фішингових листів у месенджерах.

Це вид атаки, за якого зловмисники надсилають оманливі повідомлення, що намагаються змусити користувачів до взаємодії, надаючи фальшиву інформацію чи покликання.

Наприклад, восени 2022 р. шахраї використовували месенджери WhatsApp та Telegram для того, щоб заволодіти обліковими записами користувачів. Вони пропонували фальшиві пропозиції з вакансіями та безплатну підписку на Telegram Premium. Жертви мали перейти за покликанням чи авторизуватися. У такий спосіб зловмисники отримували доступ до облікових записів.

Інструменти, що допомагають розпізнати фейкові сайти.

Google Transparency Report – цей інструмент дозволяє перевірити, чи вважає Google сайт безпечним. Він надає звіти про безпечні вебперегляди та завантаження файлів.

Web Of Trust – цей сервіс є розширенням для Google Chrome. Він оцінює вебсайти на основі відгуків користувачів та інформації про репутацію, щоб допомогти ідентифікувати ненадійні та потенційно шкідливі сайти.

VirusTotal – цей онлайн-інструмент дозволяє перевірити підозрілі файли та URL-адреси за допомогою декількох антивірусних двигунів та вебсайтів, що виявляють віруси, шкідливе програмне забезпечення та інші загрози.

ScamAdviser – цей інструмент допомагає проаналізувати інформацію стосовно домену та часу створення сайту. Користувач самостійно приймає рішення, чи є аналізований сайт фейковим.

Who.is – цей інструмент надає детальну інформацію про власників домену, включно з датою реєстрації, контактними даними та іншими важливими деталями про доменні імена.

5. Безпека в інтернеті: онлайн-репутація, шкідливий онлайн-контент, секстинг, сексторшен, кіберсталкінг.

У сучасному світі майже кожна людина стикається з онлайн-простором, спілкуючись, купуючи товари та виконуючи інші дії через інтернет. Важливо пам’ятати про безпеку в цьому середовищі. Адже там необхідно дбати про свою онлайн-репутацію, остерігатися впливу шкідливого контенту, секстингу і сексторшену та кіберсталкінгу. Все, що людина робить в інтернеті, позначається на її онлайн-репутації. А це, у свою чергу, може сильно вплинути на її життя, наприклад на кар’єру та особисті стосунки.

Для перевірки та керування власною онлайн-репутацією користувачу рекомендується:

– пошукати інформацію про себе в різних пошукових системах, використовуючи різні ідентифікаційні дані, як-от нікнейм або місце роботи;

– перевірити згадки про себе в Google Фото;

– проаналізувати свої соціальні мережі та видалити контент, який може негативно вплинути на його онлайн-репутацію.

В інтернеті можна знайти як корисну інформацію, так і шкідливу. До шкідливого онлайн-контенту відносять матеріали, які спонукають до самопошкодження чи суїциду, а також ті, що пропагують насильство, порнографію та незадоволення зовнішністю, призводячи до розладів харчової

поведінки.

Людина, яка відчуваєте вплив шкідливого онлайн-контенту, має поділитися проблемою з рідними або довіреними особами та скласти план виходу з цієї ситуації. За потреби можна звернутися до правоохоронних органів і подати скарги на вебплатформу, де розміщують такий контент; а також отримати психологічну допомогу на спеціалізованих гарячих лініях або сторінках відповідних організацій у соціальних мережах.

Важливо також знати про секстинг та сексторшен та як боротися з ними у разі, якщо людина потерпіла від цих явищ.

Секстинг – це обмін інтимними фото чи відео або ведення інтимного листування. Він може призвести до розповсюдження інтимного контенту без згоди особи та викликати сексуальне насильство, як віртуальне, так і реальне.

Сексторшен – це шантаж публікуванням сексуального контенту, щоб залякати людину чи примусити її до певних дій.

Рекомендації для користувача

Якщо хтось поширює Ваші інтимні фото чи відео без згоди:

1. Зробіть скриншоти сторінки з Вашими фото чи відео;
2. Попросіть адміністрацію соціальної мережі або сайту видалити цей контент;
3. Зверніться із заявою до правоохоронних органів та проінформуйте, що ці фото чи відео опублікували без Вашої згоди на це;
4. За секстинг і сексторшен зловмисника або зловмисницю можуть притягнути до відповідальності за статтями Кримінального кодексу України;
5. Окрім цього, за даними опитування 2017 р., 23 % жінок зазнавали кіберсталкінгу хоча б один раз за своє життя. Кіберсталкінг – це форма психологічного насильства, що характеризується переслідуванням або домаганням людини в інтернеті;
6. Для захисту зробіть скриншоти погроз та зверніться до поліції. Уникайте будь-якої комунікації з кіберсталкером чи кіберсталкеркою та поскаржтеся в соцмережах на повідомлення від такої людини. Поділіться проблемою з довіреною особою, зверніться за психологічною підтримкою, якщо маєте таку потребу.

Віртуальний світ вимагає уваги до особистої онлайн-репутації та захисту від шкідливого контенту. Перевіряйте та керуйте своєю репутацією, реагуйте на шкідливий контент та повідомлення, а за потреби звертайтеся до правоохоронних органів, аби припинити насильство у свій бік.

6. Безпека в інтернеті: кібербулінг, кібергрумінг, тролінг, флеймінг, хепіслепінг, хейтспіч, доксинг, кетфішинг.

Окрім секстингу, сексторшену та кіберсталкінгу, існує ще багато форм кібернасильства, з якими можна зіткнутися кожного дня. Ось перелік найпоширеніших.

Кібербулінг – цькування людини (найчастіше використовується в контексті дітей) через поширення образливих повідомлень або залякування у соціальних мережах. В Україні існує закон, згідно з яким булер чи булерка або їхні батьки несуть адміністративну відповідальність у виді штрафу та виправних робіт.

Кібергрумінг – входження в довіру до дитини з метою схилення її до якого-небудь брутального поводження з сексуальним підтекстом і подальшої реальної зустрічі з дитиною для сексуальних цілей.

Тролінг – розміщення в інтернеті провокаційних повідомлень. Наприклад, щоб викликати конфлікт чи взаємні образи між учасниками/учасницями розмови.

Флеймінг – обмін гнівними повідомленнями в інтернет-дискусіях.

Хепіслепінг – відеоролики, які найчастіше знімають підлітки, з записами реальних сцен насильства, в тому числі стосовно дорослих людей.

Хейтспіч (мова ворожнечі) – це агресивні висловлювання, які принижують та дискримінують людину чи групу людей за різними ознаками. Існує безліч видів мови ворожнечі, наприклад за расою, статтю чи віком.

Доксинг – збір і висвітлення у публічному просторі особистої інформації про людину, групу людей чи організацію без їхньої згоди.

Кетфішинг – створення фейкових профілів у соціальних мережах чи на сайтах для онлайн-знайомств задля обману та шахрайства або просто видавання себе за іншу людину.

Завдання:

Завдання № 1. Ознайомитися з пошуковими системами. Визначити, які пошукові системи використовувалися на початковому етапі розвитку інтернету.

1. Знайти у Google інформацію про алгоритм PageRank.

Завдання № 2. Використати Google для спеціалізованого пошуку.

1. За допомогою Google Scholar знайти 2 наукові статті з теми «OSINT-технології».
2. Використати оператор filetype:pdf для пошуку звітів із інформаційної безпеки.
3. Виконати пошук за допомогою site:gov.ua для знаходження офіційних документів.

Завдання № 3. Робота з іншими системами пошуку.

1. Використати DuckDuckGo для пошуку інформації про анонімність в інтернеті.

2. Зробити пошук тієї самої теми через Startpage та порівняти результати.

Завдання № 4. Перевірка достовірності інформації.

1. Вибрати одну новину з результатів пошуку.
2. Визначити першоджерело публікації.
3. Зіставити знайдені відомості у 2–3 різних пошукових системах.

Приклад виконання завдань № 1–4 наведено у додатку 5.

Завдання № 5. Пройти тест за темою.

Вимоги до оформлення практичної роботи

1. Загальні вимоги.

Робота виконується українською мовою.

Обсяг – 5–8 сторінок друкованого тексту (без урахування додатків).

Формат аркуша – А4; поля: верхнє та нижнє – 20 мм, ліве – 25 мм, праве – 15 мм.

Шрифт – Times New Roman, розмір – 14 пт.

Міжрядковий інтервал – 1,5.

Вирівнювання тексту – за шириною.

Абзацний відступ – 1,25 см.

2. Структура роботи.

Титульна сторінка

Назва міністерства.

Назва закладу освіти.

Назва дисципліни.

Назва практичної роботи (№, тема).

Прізвище, ім’я студента.

Група, курс.

ПІБ викладача.

Рік та місто.

Мета роботи – коротке формулювання (2–3 речення).

Завдання роботи – перелік завдань, котрі необхідно виконати.

Хід виконання роботи – опис дій здобувача: приклади пошукових запитів, результати, спостереження (можна додавати скриншоти).

Аналіз та обговорення результатів – оцінка отриманої інформації, перевірка достовірності, порівняння різних пошукових систем.

Висновки – узагальнення результатів (не менше ніж 0,5 сторінки).

Список використаних джерел – оформлюється згідно з ДСТУ 8302:2015 (оформлення бібліографічних посилань).

Додатки (за потреби) – скриншоти, таблиці, діаграми, схеми.

3. Оформлення ілюстрацій та таблиць.

Ілюстрації (схеми, графіки, скриншоти) нумеруються: *Рис. 1.1. Приклад пошукового запиту*.

Таблиці також нумеруються та мають назву: *Таблиця 1. Результати пошуку в Google*.

Посилання на рисунки та таблиці обов’язкові в тексті.

4. Вимоги до стилю викладу.

Текст має бути науково-діловим, без жаргонізмів. Використовуються чіткі, логічні формулювання. При цитуванні обов'язковим є посилання на джерело.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які етапи розвитку пошукових систем можна виокремити?
2. Чим відрізняється Google від перших пошукових систем?
3. Для чого застосовуються пошукові оператори (site:, filetype: тощо)?
4. Що таке метапошукові системи та в чому полягають їхні переваги?
5. Які системи анонімного пошуку Ви знаєте?
6. Як перевірити достовірність знайденої інформації?
7. Що таке індексація вебсторінок і як вона впливає на результати пошуку?
8. Які особливості ранжування результатів у сучасних пошукових системах?
9. Що таке Google Dork і як його можна застосовувати для пошуку інформації?
10. Які ризики та обмеження пов'язані з використанням відкритих джерел у пошуку інформації?

ЗАПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ»

1. Які основні можливості надає штучний інтелект у правозастосуванні?
2. Наведіть приклади сучасних інструментів AI, що використовуються для аналізу правової інформації.
3. У чому полягає перевага автоматизації юридичних досліджень?
4. Які ризики пов’язані з використанням AI у прогнозуванні судових рішень?
5. Які етичні виклики виникають при впровадженні AI у правову діяльність?
6. Чому штучний інтелект не може повністю замінити суддю або адвоката?
7. Наведіть приклад ситуації, коли алгоритм AI може допустити упереджене рішення.
8. Які міжнародні регуляторні обмеження застосовуються до використання AI у праві?
9. Що таке електронні докази?
10. Які вимоги висуваються до допустимості електронних доказів у суді?
11. Які методи цифрової криміналістики застосовуються для відновлення видалених файлів?
12. Як забезпечується автентичність електронного документа?
13. У чому полягають відмінності використання цифрових доказів у кримінальному та цивільному процесах?
14. Наведіть приклад судової практики України щодо використання електронних доказів.
15. Які міжнародні стандарти регулюють цифрові докази (наприклад, Будапештська конвенція)?
16. Якими є основні ризики маніпуляції цифровими доказами?
17. Як можна визначити поняття «адвокатська таємниця» в контексті кібербезпеки?
18. Якими є основні технічні методи захисту електронної комунікації між адвокатом і клієнтом?
19. Поясніть принцип роботи шифрування даних.
20. Які існують засоби безпечного зберігання правової інформації?
21. Які організаційні заходи вживаються в юридичній фірмі для запобігання витоку даних?
22. Хто несе відповідальність за витік конфіденційної інформації з адвокатської контори?
23. Наведіть приклади відомих кіберінцидентів, пов’язаних із

юридичними даними.

24. Які правові наслідки може мати порушення кібербезпеки у сфері адвокатської діяльності?

25. Що таке електронне правосуддя?

26. Які функції виконує Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) в Україні?

27. Якими є основні переваги електронного правосуддя для учасників процесу?

28. Що таке ODR і в яких випадках воно застосовується?

29. Який міжнародний досвід онлайн-арбітражу може бути корисним для України?

30. Які технічні та соціальні виклики існують при впровадженні електронного правосуддя?

СПИСОК ОСНОВНОЇ ЛІТЕРАТУРИ ДО НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ»

Нормативно-правові акти

Закони України, міжнародно-правові акти

1. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. Ратифікована Законом України від 17.07.1997. URL : https://zakon.rada.gov.ua/laws/show/995_004#Text.
2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text.
3. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012. URL : https://zakon.rada.gov.ua/laws/show/5076-17#Text.
4. Про електронні документи та електронний документообіг : Закон України від 22.05.2003. URL : https://zakon.rada.gov.ua/laws/show/851-15#Text.
5. Про захист персональних даних : Закон України від 01.06.2010. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Про інформацію : Закон України від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.
7. Цивільний процесуальний кодекс України : Закон України від 18.03.2004. URL : https://zakon.rada.gov.ua/laws/show/1618-15.
8. 78/213. Promotion and protection of human rights in the context of digital technologies : Resolution adopted by the General Assembly on 19 December 2023. *United Nations.* URL : https://docs.un.org/en/A/RES/78/213.
9. Canada launches first-ever Artificial Intelligence Strategy for the federal public service. *Government of Canada.* URL : https://www.canada.ca/en/treasury-board-secretariat/news/2025/03/canada-launches-first-ever-artificial-intelligence-strategy-for-the-federal-public-service.html.
10. ISO/IEC 27037:2012. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence. *ISO.* URL : https://www.iso.org/standard/44381.html.
11. ISO/IEC 27042:2015. Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence. *ISO.* URL : https://www.iso.org/standard/44406.html.
12. ISO/IEC 27043:2015. Information technology. Security techniques. Incident investigation principles and processes. *ISO.* URL : https://www.iso.org/standard/44407.html.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL : https://eur-lex.europa.eu/eli/reg/2016/679/oj.

14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL : https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Підзаконні нормативні акти

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 08.02.2021 № 92. URL : https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text.

2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 03.08.2017 № 676. URL : https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

3. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL : https://zakon.rada.gov.ua/go/1556-2020-%D1%80.

Підручники

1. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційні технології : підруч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 492 с.

2. Інформаційні системи та технології : підруч. / кол. авт. ; за заг. ред. В. Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с.

Навчальні посібники, інші дидактичні та методичні матеріали

1. Бакаянова Н. М., Кубаєнко А. В., Кісліцина І. О. Сучасна концепція реформування судоустрою, судочинства та суміжних правових інститутів : навч.-метод. посібник (для здоб. ступеня д-ра філос. денної, вечірньої та заочної форми навч.). Одеса: Фенікс, 2021. 157 с.

2. Бутенко Т. А. Сирий В. М. Інформаційні системи та технології : навч. посібник. Харків : ХНАУ ім. В. В. Докучаєва, 2020. 207 с.

3. Гавриш О. С., Махницький О. В., Прокопов С. О., Рижков Е. В. Захист інформаційних ресурсів підрозділів Національної поліції місцевого рівня : метод. рекомендації. Дніпро : Дніпроп. держ. ун-т. внутр. справ, 2018. 34 с.

4. Гребенюк А. М., Рижков Е. В., Синиціна Ю. П., Прокопов С. О. Інформаційні та комунікаційні технології : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 337 с.

5. Ковальова О. В. Інформаційне забезпечення професійної діяльності :

навч. посібник. Київ : Дакор, 2021. 288 с.

6. Кормич Б. А., Федотов О. П., Аверочкіна Т. В. Правове регулювання інформаційної діяльності : навч.-метод. посібник. Одеса : Одеська юридична академія, 2018. 150 с.

7. Косиченко О. О., Махницький О. В. Інформаційне забезпечення юридичної діяльності : посібник. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 205 с.

8. Павлиш В. А., Гліненко Л. К., Шаховська Н. Б. Основи інформаційних технологій і систем : підруч. Львів : Видавництво Львівської політехніки, 2018. 620 с.

9. Рижков Е. В., Синиціна Ю. П., Прокопов С. О. та ін. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посібник. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с.

10. Чумаков А. Г. Інформаційні системи і технології у фінансах : навч. посібник. Дніпро : ФОП Дробязко С. І., 2018. 174 с.

Монографії та інші наукові видання

1. Мирошниченко В. О., Прокопов С.О., Рижков Е. В. Впровадження сучасних систем цифрового радіозв'язку у підрозділах Національної поліції : наук.-практ. рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 29 с.

2. Синиціна Ю. П. Автоматизовані інформаційні системи в правоохоронній діяльності. *Економічна та інформаційна безпека: актуальні питання та інновації : матеріали Всеукр. наук.-практ. конф.* (м. Дніпро, 04 лист. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. С. 220–222.

3. Синиціна Ю. П. APT-атак – пріоритетний напрямок розвитку кібербезпеки. *Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф.* (м. Львів, 19 груд. 2020 р.). Львів : ЛьвДУВС, 2020. С. 66–68.

4. Синиціна Ю. П. Державне управління забезпечення національної безпеки: інформаційна безпека. *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VI Міжнар. наук.-практ. конф.* (м. Дніпро, 11 бер. 2022 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. С. 266–269.

5. Синиціна Ю. П. Інформаційна безпека у системі права національної безпеки України. *Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об'єктів права інтелектуальної власності : зб. наук. праць за матеріалами IV Міжнар. наук.-практ. інтернет-конф.* (м. Київ, Дніпро, 24-25 бер. 2022р.). Дніпро : Юрсервіс, 2022. С. 165–168.

6. Синиціна Ю. П. Сучасні підходи до безпеки операційних систем. *Сучасні інформаційні технології в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару* (м. Дніпро, 26 лист. 2020 р.). Дніпро :

Дніпроп. держ. ун-т внутр. справ, 2020. С. 66–68.

7. Синиціна Ю. П., Бекишев А. К. Методологічні аспекти цифрової комунікації закладів вищої освіти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2021. № 3 (112). С. 340–348.

8. Синиціна Ю. П., Дудуник В. В. Актуальні питання взаємозв'язку інформаційної та національної безпеки України. *Сучасні інформаційні технології в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару* (м. Дніпро, 26 лист. 2020 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. С. 164–167.

9. Синиціна Ю. П., Кліменко А. О. Актуальні питання інформаційної безпеки в діяльності Національної поліції України. *Сучасні інформаційні технології в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару* (м. Дніпро, 26 лист. 2020 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. С. 174–176.

10. Синиціна Ю. П., Причина В. Р. Оцінка системи управління інформаційної безпеки методом таксономії. *Nauka i edukacja w warunkach zmian cywilizacyjnych : Mater. II Międz. Konf. Nauk.-Prakt.* (Łódź, 31 października 2020 r.). Łódź: Nowa nauka, 2020. S. 76–78.

11. Синиціна Ю. П., Рижков Е. В., Станіна О. Д. Штучний інтелект: що змінилося за 50 років // Theoretical foundations of engineering. Tasks and problems : collective monograph / Boiko T., Boiko P., etc. Boston : International Science Group ; Primedia eLaunch, 2021. 485 p. P. 341–348.

12. Синиціна Ю. П., Станіна О. Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Synytsina Yu., Stanina O. Rationale for the relevance of digital communication in higher education institutions) // Selected aspects of digital society development : monograph / ed. by T. Nestorenko and A. Ostenda. Katowice : Publishing House of University of Technology, 2021. 260 s. S. 148–156.

Інші джерела

1. Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. *ACLU of Massachusetts.* URL : https://data.aclum.org/storage/2025/01/OSTP_www_whitehouse_gov_ostp_ai-bill-of-rights.pdf.

2. Ethics guidelines for trustworthy AI. *European Commission.* URL : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

3. Guidelines for prosecutors on digital evidence collection in compliance with international standards on freedom of expression and privacy. *UNESCO.* URL : https://unesdoc.unesco.org/ark:/48223/pf0000395060.

4. Recommendation on the Ethics of Artificial Intelligence. *UNESCO.* URL : https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

5. The 17 Goals (Sustainable Development Goals). *United Nations*. URL : https://sdgs.un.org/goals.

Інтернет-ресурси

1. Єдиний державний веб-портал відкритих даних. URL : https://data.gov.ua/.
2. Інформаційно-пошукова правова система «Нормативні акти України» (НАУ). URL : http://www.nau.ua.
3. Міністерство внутрішніх справ України. URL : https://www.mvs.gov.ua/.
4. Наукова бібліотека Харківського національного університету внутрішніх справ. URL : https://lib.univd.edu.ua/.
5. Національна поліція України. URL : https://www.npu.gov.ua/.

СИСТЕМА ОЦІНЮВАННЯ УСПІШНОСТІ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ»

Для навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності» засобами діагностики знань (успішності навчання) виступають: лекційні, семінарські та практичні заняття, самостійна робота і підсумковий контроль.

<table>
<tr><td colspan="3">ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ</td></tr>
<tr><td colspan="2">Поточний контроль (ПК)</td><td>Підсумковий контроль</td></tr>
<tr><td>Аудиторна робота</td><td>Самостійна робота/ Індивідуальна робота</td><td rowspan="2">Залік (З) / ЕКЗАМЕН (Е)</td></tr>
<tr><td>≤ 20</td><td>≤ 30</td></tr>
<tr><td colspan="2">≤ 50</td><td>≤ 50</td></tr>
<tr><td colspan="3">Підсумкова оцінка у випадку заліку (П) ПК + З ≤ 100</td></tr>
<tr><td colspan="3">Підсумкова оцінка у випадку складання екзамену (П) ПК + Е ≤ 100</td></tr>
</table>

Критерієм успішного проходження здобувачем підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Мінімальний пороговий рівень оцінки визначається за допомогою якісних критеріїв і трансформується в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Здобувач допускається до складання підсумкового контролю, якщо ним виконані всі передбачені РПНД поточні завдання та сума балів поточного контролю становить не менше ніж 34. Якщо сума балів поточного контролю є меншою за 34, здобувач не допускається до підсумкового контролю і зобов’язаний доопрацювати завдання та набрати необхідну кількість балів.

За результатами аудиторної роботи здобувач заочної форми навчання може отримати як максимальну кількість 20 балів (кожне заняття оцінюється за п’ятибальною шкалою); за результатами самостійної роботи – 30 балів. Таким чином, показник балів за поточний контроль складає 34–50 балів.

Розрахунок підсумкової оцінки з навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності» здійснюється відповідно до формули:

$$\mathbf{П\ ПК+З\leq 100,}$$

де ПК – бали за поточний контроль (34–50 балів),

З – бали за результатами складання заліку.

Критерії оцінювання аудиторної роботи здобувачів вищої освіти (заочної форми навчання)

БАЛИ	ПОЯСНЕННЯ
5	**Високий рівень** компетентностей. Питання, винесені на розгляд, **засвоєні у повному обсязі; на високому рівні сформовані** необхідні практичні навички та вміння; **всі** навчальні завдання, передбачені планом заняття, **виконані** в повному обсязі. Під час заняття продемонстрована стабільна активність та ініціативність. Відповіді на теоретичні запитання, виконання практичних завдань, висловлення власної думки стосовно дискусійних питань ґрунтується **на глибокому знанні** чинного законодавства, теорії та правозастосовної практики.
4	**Невисокий рівень** компетентностей. Питання, винесені на розгляд, **засвоєні у повному обсязі; загалом сформовані** необхідні практичні навички та вміння; **всі** передбачені планом заняття навчальні завдання **виконані** в повному обсязі **з неістотними неточностями**. Під час заняття продемонстрована ініціативність. Відповіді на запитання, виконання практичних завдань, висловлення власної думки стосовно дискусійних питань **переважно ґрунтується на знанні** чинного законодавства, теорії та правозастосовної практики.
3	**Достатній рівень** компетентностей. Питання, винесені на розгляд, **загалом засвоєні**; практичні навички та вміння мають **поверхневий характер**, потребують подальшого напрацювання та закріплення; навчальні завдання, передбачені планом заняття, **виконані**, **деякі** види завдань виконані **з помилками**.
2	**Недостатній рівень** компетентностей. Питання, винесені на розгляд, **засвоєні частково**, **прогалини** у знаннях **не мають істотного характеру**; практичні навички та вміння **сформовані недостатньо**; **більшість** навчальних завдань **виконано, деякі** з виконаних завдань **містять істотні помилки,** які потребують подальшого усунення.
1	**Мінімальний рівень** компетентностей. Студент не готовий до заняття, не знає більшої частини програмного матеріалу, з труднощами виконує завдання, невпевнено відтворює терміни і поняття, що розглядалися під час заняття, допускає змістовні помилки, не володіє відповідними вміннями і навичками, необхідними для виконання професійних завдань.
0	**Незадовільний рівень** компетентностей. Відсутність на занятті.

Для навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності» засобами діагностики знань (успішності навчання) виступають: стандартизовані тести, тези, есе, презентації результатів

виконаних завдань та досліджень, презентації та виступи на наукових заходах, інші види індивідуальних та групових завдань.

Критерії оцінювання самостійної роботи

(заочна форма навчання)

Пропонується таке оцінювання самостійної роботи здобувачів вищої освіти за виконання 1 завдання за вибором здобувача та узгодженням із викладачем для отримання максимальної кількості балів – 30:

1. Підготовка роботи та участь у конкурсі творчих та/або наукових робіт серед здобувачів (МОН України, ДДУВС) (написання робіт, есе, доповідь, творча публікація, творча візуалізація, відеоролик) – 30 балів;
2. Підготовка презентацій-доповідей для участі в роботі наукового студентського гуртка кафедри (надати презентацію та фото виступу) – 30 балів;
3. Підготовка тез доповіді на міжнародну (всеукраїнську) науково-практичну конференцію за умови надання Print Screen перевірки на плагіат із результатом не менше 70 % оригінального тексту. Тези повинні бути підготовленні відповідно до Методичних вказівок з написання тез – 30 балів;
4. Отримання сертифікату після проходження онлайн-тесту «Цифроґрам 1.0 для громадян» на платформі «Дія.Освіта» https://osvita.diia.gov.ua/digigram – 30 балів;
5. Підготовка презентації у редакторі «Google Презентації» (завантаження презентації та надання посилання у коментарях) за темою зі списку у додатковому файлі «Методичні вказівки до виконання презентації у редакторі Гугл презентація» – 30 балів;
6. Проходження тесту з самостійної роботи – 30 балів.

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ECTS	
	Залік	Екзамен/ диференційований залік	Оцінка	Пояснення
90–100	зараховано	Відмінно	A	«**Відмінно**» – теоретичний зміст курсу засвоєний у повному обсязі; сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані в повному обсязі.
83–89		Добре	B	«**Дуже добре**» – теоретичний зміст курсу засвоєний в повному обсязі; загалом сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання більшості з них оцінена кількістю балів, що є близькою до максимальної.
75–82			C	«**Добре**» – теоретичний зміст курсу засвоєний цілком; загалом сформовані практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання жодного з них не оцінена мінімальною кількістю балів, деякі види завдань виконані з помилками.
68–74		Задовільно	D	«**Задовільно**» – теоретичний зміст курсу засвоєний не повністю, але прогалини не мають істотного характеру; загалом сформовані необхідні практичні навички роботи із засвоєним матеріалом; більшість передбачених РПНД навчальних завдань виконано, деякі з виконаних завдань містять помилки.

60–67			E	«**Достатньо**» – теоретичний зміст курсу засвоєний частково; не сформовано деякі практичні навички роботи; частина передбачених РПНД навчальних завдань не виконана або якість виконання деяких із них оцінена кількістю балів, що є близькою до мінімальної.
35–59	не зараховано	Незадовільно	FX	«**Умовно незадовільно**» – теоретичний зміст курсу засвоєний частково; не сформовані необхідні практичні навички роботи; більшість навчальних завдань не виконано або якість їх виконання оцінено кількістю балів, що є близькою до мінімальної; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (із можливістю повторного складання).
1–34			F	«**Безумовно незадовільно**» – теоретичний зміст курсу не засвоєний; не сформовані необхідні практичні навички роботи; всі виконані навчальні завдання містять грубі помилки або не виконані взагалі; додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань.

СЛОВНИК ТЕРМІНІВ

ТЕМА 1. Використання штучного інтелекту в правозастосовній практиці: можливості, ризики та етичні виклики.

Автоматизований правовий аналіз – використання AI для аналізу законодавства, судових рішень і договорів.

Алгоритмізація – процес формалізації та впровадження алгоритмів для вирішення юридичних завдань.

Етичні виклики – проблеми, що виникають через застосування AI: упередженість, прозорість, конфіденційність.

Кібербезпека – комплекс заходів для захисту правових даних та інформаційних систем від несанкціонованого доступу.

Машинне навчання (Machine Learning, ML) – підрозділ AI, що дозволяє комп'ютерним системам «навчатися» на основі даних та покращувати свої результати без прямого програмування.

Правова відповідальність AI – питання визначення суб'єкта відповідальності за дії, вчинені з використанням штучного інтелекту.

Правова експертиза з AI – оцінка правових документів і процесів із використанням інтелектуальних систем.

Правозастосування – практична діяльність органів влади та судів із реалізації норм права.

Прогнозування судових рішень – застосування AI для оцінки ймовірності прийняття певного рішення судом.

Штучний інтелект (Artificial Intelligence, AI) – галузь комп'ютерних наук, що створює системи, здатні виконувати завдання, які зазвичай потребують людського інтелекту (аналіз, прогнозування, розпізнавання образів).

ТЕМА 2. Цифрова доказова база у кримінальному та цивільному процесах: збір, збереження та допустимість.

Автентичність доказу – підтвердження, що електронний документ не був змінений та походить від зазначеного джерела.

Допустимість доказу – відповідність електронного доказу вимогам процесуального законодавства щодо способу отримання та подання.

Електронне листування – електронні листи, повідомлення у месенджерах чи соціальних мережах, що можуть бути подані як докази у суді.

Електронний доказ – будь-яка інформація в цифровій формі (електронні документи, листування, метадані тощо), що може бути використана в суді як доказ.

Електронний документ – документ, створений у цифровій формі та підписаний електронним підписом, що має юридичну силу.

Кваліфікований електронний підпис (КЕП) – засіб автентифікації, що прирівнюється до власноручного підпису та підтверджує цілісність

документа.

Ланцюг збереження (Chain of custody) – документування всіх етапів збору, передачі та зберігання електронних доказів для гарантії їхньої цілісності.

Метадані – технічна інформація про електронний файл (дата створення, автор, місце збереження, історія змін), що може підтвердити його автентичність.

Цифрова криміналістика (Digital forensics) – галузь знань і практики, спрямована на виявлення, збирання, аналіз і збереження електронних доказів.

Цифровий слід – сукупність даних, які залишає користувач під час взаємодії з інформаційними системами (IP-адреси, лог-файли, геолокація).

ТЕМА 3. Кібербезпека юридичних даних: методи та стратегії інформаційної безпеки.

Володілець персональних даних – фізична чи юридична особа, яка визначає мету і порядок обробки персональних даних.

Захист персональних даних – комплекс організаційних і технічних заходів, спрямованих на запобігання несанкціонованому доступу, зміні, втраті чи поширенню персональної інформації.

Згода на обробку персональних даних – добровільне волевиявлення суб'єкта даних, яке надається для їх обробки в певній формі (усній, письмовій, електронній).

Конфіденційність – гарантія того, що персональні дані доступні лише тим особам, які мають на це законне право та необхідність.

Обробка персональних даних – будь-яка дія або сукупність дій щодо персональних даних (збирання, зберігання, використання, поширення, знищення тощо).

Персональні дані – будь-яка інформація, що прямо або опосередковано дозволяє ідентифікувати фізичну особу (наприклад: ПІБ, дата народження, адреса, телефон, електронна пошта).

Право на забуття – право суб'єкта персональних даних вимагати від володільця їх видалення у випадках, передбачених законодавством.

Розпорядник персональних даних – особа, якій володілець передає право обробки персональних даних на законних підставах.

Суб'єкт персональних даних – фізична особа, стосовно якої здійснюється обробка її персональних даних.

Чутливі персональні дані – категорія даних, що потребує особливого захисту (наприклад: стан здоров'я, біометричні та генетичні дані, політичні чи релігійні переконання).

ТЕМА 4. Пошук правової інформації в мережі інтернет. особиста безпека в інтернеті.

Анонімізація – методи приховування особистих даних і діяльності користувача в мережі (VPN, TOR, проксі-сервери).

Достовірність джерела – показник надійності та точності отриманої з відкритих ресурсів інформації, який перевіряється шляхом порівняння кількох незалежних джерел.

Кібергігієна – комплекс правил безпечної поведінки в Інтернеті: використання надійних паролів, двофакторної автентифікації, перевірка посилань тощо.

Метапошукова система – сервіс, що одночасно використовує кілька пошукових систем і видає зведені результати (наприклад, StartPage, DuckDuckGo).

Пошукова система – спеціалізований програмний комплекс для пошуку інформації в мережі Інтернет (наприклад, Google, Bing, Yahoo).

Соціальна інженерія – психологічні методи маніпуляцій для отримання конфіденційної інформації від користувачів.

Спеціалізований пошук (Advanced Search) – використання логічних операторів та фільтрів для точнішого пошуку даних.

Фішинг (Phishing) – вид кіберзлочину, що полягає у викраденні особистих даних шляхом маскування під надійні сервіси чи організації.

Цифровий слід (Digital footprint) – інформація, яку користувач залишає про себе в інтернеті (пости, фото, коментарі, історія пошуку тощо).

OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел, тобто пошук, збір і аналіз інформації, яка є у вільному доступі.

Додаток 1

ПРИКЛАД ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ. ТЕМА № 1

Тема: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВОЗАСТОСОВНІЙ ПРАКТИЦІ: МОЖЛИВОСТІ, РИЗИКИ ТА ЕТИЧНІ ВИКЛИКИ.

Мета: ознайомитися з сучасними AI-інструментами для правового пошуку, протестувати їхню ефективність та порівняти з традиційними базами даних.

Хід виконання роботи

Крок 1. Вибір інструментів.

Для тестування обрано:

1. ChatGPT (AI-модель загального призначення з можливістю юридичного пошуку);
2. CaseText CoCounsel (спеціалізований AI-юрист, працює з американським правом);
3. Єдиний державний реєстр судових рішень України – традиційна база даних.

Крок 2. Формування правового запиту.

Запит для тестування: «Якими є порядок та підстави розірвання договору оренди нежитлового приміщення за законодавством України?».

Крок 3. Робота з AI-сервісами.

1. ChatGPT.

Результат:

1) надано огляд норм Цивільного кодексу України (ст. 651, 782, 783, 785);

2) описано загальні підстави: істотне порушення умов, невиконання зобов'язань, неможливість використання приміщення;

3) запропоновано кроки розірвання договору в судовому та позасудовому порядку.

2. CaseText CoCounsel.

Результат:

1) зважаючи на те, що сервіс орієнтований на США, він не надав актуальних норм українського права;

2) запропоновано алгоритм розірвання на основі загальних принципів договірного права;

3) виявлено обмеження застосування до нашої юрисдикції.

Крок 4. Робота з традиційною базою даних.

ЄДРСР.

Результат:

1) знайдено 12 рішень судів щодо розірвання договору оренди нежитлового приміщення. Два з них містили повний аналіз норм права та обґрунтування;

2) інформація безпосередньо підтверджена судовою практикою, але потребувала часу на пошук і відбір.

Крок 5. Порівняння результатів.

Критерій	**ChatGPT**	**CaseText CoCounsel**	**ЄДРСР**
Швидкість пошуку	Висока	Висока	Низька
Актуальність норм	Висока	Низька	Висока
Повнота відповіді	Висока	Середня	Висока
Потреба у перевірці	Висока	Висока	Низька
Зручність інтерфейсу	Висока	Висока	Середня

Висновки.

1. ChatGPT – зручний для швидкого орієнтування у правовій темі, але потребує перевірки посилань на норми.
2. CaseText – корисний для англомовних юрисдикцій, але малопридатний для українського права.
3. ЄДРСР – найточніше джерело офіційної судової практики, але менш зручне у швидкому пошуку.

Рекомендації.

1. Використовувати AI-сервіси як додатковий інструмент для попереднього аналізу, але перевіряти отриману інформацію у нормативних актах і судових рішеннях.
2. Поєднувати швидкість AI та достовірність офіційних баз.

Додаток 2

КЕЙСИ ДО ПРАКТИЧНОЇ РОБОТИ. ТЕМА № 2

Кейс 1.

Ситуація: ФОП Іваненко подав позов до ТОВ «Гамма» про розірвання договору підряду. Як докази позивач надав:

– листування корпоративною електронною поштою;
– аудіозапис телефонної розмови, зроблений на мобільний телефон;
– фото пошкодженого об’єкта, надіслані у Viber.

Заперечення відповідача:

– аудіозапис здійснено без згоди;
– фото не містять метаданих;
– відсутнє підтвердження автентичності електронних листів.

Кейс 2.

Ситуація: ТОВ «Омега» вимагає визнати недійсним договір, укладений шляхом обміну сканами.

Докази:

– PDF-копії договору з підписами, надіслані електронною поштою;
– листування у WhatsApp щодо погодження умов.

Заперечення відповідача:

– підпис на сканах не перевірено;
– листування у месенджері не підтверджене експертизою.

Кейс 3.

Ситуація: ФОП Петренко подав позов про стягнення боргу за послуги.

Докази:

– звіт з CRM-системи про виконані роботи;
– листи на електронну пошту клієнта;
– відеозапис демонстрації послуги, збережений у «хмарі».

Заперечення відповідача:

– CRM-звіт можна редагувати;
– листи не мають цифрового підпису;
– відео не містить даних про дату створення.

Кейс 4.

Ситуація: ТОВ «Сигма» подало позов про відшкодування збитків.

Докази:

– скриншоти банківських повідомлень з мобільного застосунку;
– листування у Facebook Messenger;
– файл Excel з розрахунком збитків.

Заперечення відповідача:

– скриншоти легко підробити;
– листування в соцмережі не автентифіковане;
– файл Excel можна редагувати без сліду.

Кейс 5.

Ситуація: ФОП Сидоренко подав позов про захист ділової репутації.

Докази:

– пости у Twitter, що містять образи;
– скриншоти коментарів у Facebook;
– збережена копія вебсторінки через web.archive.org.

Заперечення відповідача:

– не доведено, що акаунт належить відповідачу;
– скриншоти не містять технічних даних;
– web.archive.org не є офіційним джерелом доказів.

Кейс 6.

Ситуація: ТОВ «АгроТех» судиться з постачальником через неякісну продукцію.

Докази:

– листування у корпоративному чаті у Slack;
– фото продукції з мобільного телефону;
– електронна товарно-транспортна накладна (е-ТТН).

Заперечення відповідача:

– дані в Slack могли бути видалені або змінені;
– фото не має прив’язки до часу та місця;
– е-ТТН не підписана належним КЕП.

Кейс 7.

Ситуація: ФОП Коваленко подає позов про невиплату гонорару.

Докази:

– листування у Telegram з погодженням розміру оплати;
– платіжні квитанції у PDF;
– збережені повідомлення з Google Chat.

Заперечення відповідача:

– Telegram-листування не засвідчене;
– PDF-квитанції без електронного підпису банку;
– Google Chat не є офіційним каналом комунікації.

Кейс 8.

Ситуація: ТОВ «БудПро» оскаржує відмову у гарантійному ремонті.

Докази:

– відеозапис дефекту, надісланий електронною поштою;
– листування у корпоративному порталі;

– фото накладної з мобільного телефону.

Заперечення відповідача:

– відео можна змонтувати;
– дані з корпоративного порталу можна редагувати;
– фото не має підтвердження дати створення.

Кейс 9.

Ситуація: ФОП Гринь подає позов про незаконне використання фотографій.

Докази:

– скриншоти сайту відповідача з розміщеними фото;
– листування за допомогою Instagram Direct;
– метадані оригінальних знімків.

Заперечення відповідача:

– сайт міг бути підроблений;
– Instagram Direct не є офіційним доказом;
– метадані можна змінити.

Кейс 10.

Ситуація: ТОВ «ЕкоСвіт» вимагає повернути передоплату за непоставлений товар.

Докази:

– скриншоти банківських переказів з мобільного застосунку;
– листування у Skype;
– файл PDF з рахунком-фактурою.

Заперечення відповідача:

– скриншоти не засвідчені банком;
– Skype-листування можна видалити;
– файл PDF без КЕП не є достатнім підтвердженням.

Додаток 3

ПРИКЛАД ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ. ТЕМА № 2

Крок 1. Вибір кейсу для аналізу.

Ситуація: ТОВ «Альфа» подало позов до ПП «Бета» про стягнення заборгованості за договором поставки. Як докази позивач надав:

1. Листування електронною поштою з відповідачем.
2. Скриншоти листування у месенджері Telegram.
3. Електронну копію договору у форматі PDF, підписану КЕП.

Відповідач заперечує допустимість частини доказів, стверджуючи, що:

– скриншоти можуть бути змонтованими;
– немає підтвердження автентичності e-mail;
– листування в месенджері не засвідчене в належний спосіб.

Крок 2. Визначення допустимості доказів.

Вид доказу	**Нормативне регулювання (ЦПК України, Закони України «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги»)**	**Оцінка допустимості**
Електронна пошта	Може бути доказом, якщо є технічні дані про відправника, час та цілісність повідомлення (збереження заголовків e-mail).	Є допустимим за наявності технічної експертизи
Скриншоти месенджера	Самі собою не гарантують автентичність. Потрібне підтвердження з боку адміністратора сервісу або нотаріальне засвідчення.	Сумнівна допустимість
PDF-договір із КЕП	Є електронним документом з належним підписом, підтвердженим сертифікатом.	Є допустимим

Крок 3. Виявлення помилок при зборі або поданні доказів.

1. Скриншоти месенджера не були підтверджені шляхом запиту до адміністратора Telegram або нотаріального засвідчення.

2. Електронні листи були подані у вигляді текстових файлів без заголовків та технічних метаданих.

3. Не було проведено експертизи електронних доказів на предмет цілісності.

Крок 4. Обговорення можливих стратегій захисту.

Для позивача:

– подати запит до провайдера e-mail для підтвердження автентичності

листів;

– засвідчити скриншоти у нотаріуса або отримати відповідь від адміністрації месенджера;

– замовити технічну експертизу електронних файлів.

Для відповідача:

– оскаржувати допустимість електронних доказів через відсутність належного підтвердження;

– звернути увагу суду на можливість редагування скриншотів;

– підкреслити відсутність безперервного ланцюга збереження доказів.

Додаток 4

Таблиця 1

Ризики обробки персональних даних та заходи їх мінімізації

№	Потенційний ризик	Приклад ситуації	Наслідки	Заходи мінімізації
1	Несанкціонований доступ	Злом акаунта електронної пошти юриста	Викрадення конфіденційної інформації	Використання двофакторної автентифікації, регулярна зміна паролів
2	Витік даних через людський фактор	Працівник випадково переслав клієнтські дані сторонній особі	Порушення конфіденційності, юридична відповідальність	Навчання персоналу, впровадження політики доступу «мінімально необхідний»
3	Кібератака (фішинг, віруси)	Перехід за шкідливим покликанням у листі	Втрата або блокування даних	Використання антивірусного ПЗ, VPN, кібергігієна
4	Використання слабких паролів	Пароль на кшталт «123456»	Легкий підбір пароля зловмисником	Політика складних паролів, менеджери паролів
5	Недостатнє шифрування даних	Збереження клієнтських документів у незахищеному вигляді	Перехоплення даних при передачі	Використання SSL/TLS, шифрування баз даних та файлів
6	Втрата носія з даними	Загублений ноутбук чи флешка з інформацією	Доступ третіх осіб до конфіденційних файлів	Шифрування дисків, захищені хмарні сервіси, віддалене блокування
7	Збирання надмірних даних	Зберігання копій паспортів без потреби	Зайві ризики при витоку	Мінімізація оброблюваних даних (data minimization)
8	Недостатній контроль доступу	Усі співробітники мають доступ до всієї бази	Підвищення ризику внутрішніх витоків	Розмежування прав доступу, аудит дій користувачів
9	Відсутність резервного копіювання	Втрата даних через збій системи	Неможливість відновлення клієнтських справ	Регулярне створення резервних копій у захищених сховищах
10	Невідповідність законодавству	Обробка даних без згоди суб’єкта	Адміністративна та кримінальна відповідальність	Дотримання положень Закону України «Про захист персональних даних» та GDPR

Додаток 5

ПРИКЛАД ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ. ТЕМА № 4

Тема: ПОШУК ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА В ІНТЕРНЕТІ.

Мета: ознайомитися з історією розвитку пошукових систем, навчитися користуватися базовими та спеціалізованими інструментами Google, а також перевіряти достовірність знайденої інформації.

Хід виконання роботи

Завдання 1. Ознайомлення з пошуковими системами.

1. Перші пошукові системи: Archie (1990), Lycos (1994), AltaVista (1995), Yahoo (1995).

2. У Google знайдено інформацію про PageRank – алгоритм, що оцінює значущість вебсторінки на основі кількості та якості посилань.

Завдання 2. Використання Google для спеціалізованого пошуку.

1. Google Scholar:

Запит: «OSINT technologies».

Знайдено статті:

«Open Source Intelligence (OSINT) in Cybersecurity» (2021);

«The Role of OSINT in Modern Security Analysis» (2020).

2. Пошук у Google за допомогою оператора filetype:.

Запит: OSINT filetype:pdf.

Результат: «OSINT Tools and Techniques Report.pdf» (аналітичний звіт).

3. Пошук за допомогою site:.

Запит: OSINT site:gov.ua.

Результат: публікації Міністерства цифрової трансформації України, новини CERT-UA.

Завдання 3. Робота з іншими системами пошуку.

1. У DuckDuckGo за запитом «Internet anonymity» знайдено статті про VPN, Tor, анонімний пошук.

2. У Startpage за тим самим запитом результати були подібними, але з додатковим акцентом на інструменти шифрування та захисту даних.

Завдання 4. Перевірка достовірності інформації.

1. Вибрано новину з Facebook: *«У місті Х зупинили метро через технічні несправності»*.

2. Перевірка.

Google News – підтверджено, що метро дійсно не працювало у зазначений час.

Telegram-канали – з’явилася інформація з офіційного джерела міської ради.

Висновок: інформація достовірна, але перше повідомлення було подане у перебільшеній формі.

ВИСНОВКИ: Історія пошукових систем свідчить про еволюцію від простих каталогів до інтелектуальних алгоритмів Google. Оператори пошуку значно спрощують знаходження потрібних матеріалів. Метапошуковики (Startpage, Dogpile) надають більш широкий спектр результатів, а DuckDuckGo корисний для анонімного пошуку. Перевірка достовірності інформації вимагає зіставлення кількох незалежних джерел.

РЕКОМЕНДАЦІЇ З ОСОБИСТОЇ БЕЗПЕКИ В ІНТЕРНЕТІ

1. Завжди пам’ятайте про свою приватність. Не надавайте людям, з якими знайомитися, конфіденційну інформацію. Наприклад, у жодному разі не повідомляйте свої паспортні дані.
2. Перевірте людину у «чорних списках» аферистів – їх можна знайти у відкритому доступі в мережі. Наприклад, у фейсбуці чи на вебсайті «База шахраїв України».
3. Якщо людина, з якою Ви спілкуєтеся на сайті знайомств, викликає у Вас підозри чи дискомфорт, краще з самого початку припинити комунікацію з нею.
4. Намагайтеся поспілкуватися за допомогою відеозв’язку. Як правило, аферисти не бажають показувати власне обличчя, тому це є чудовою перевіркою.
5. Якщо Ви вирішили піти на побачення з людиною із сайту знайомств, обов’язково виберіть людне місце, яке Ви добре знаєте, та заплануйте зустріч у денний час.
6. Повідомте людям, яким довіряєте, про місце зустрічі та надайте інформацію про людину, з якою йдете на це побачення. Якщо план раптово змінюється, то теж краще повідомити про це тих, кому довіряєте.
7. Якщо відчуваєте небезпеку, то одразу припиняйте зустріч та викликайте поліцію за номером 102.
8. Пам’ятайте, що людина, з якою Ви спілкуєтеся в інтернеті, не завжди в реальному житті відповідає своєму віртуальному образу.
9. Перевіряйте покликання, які вам надсилає незнайома людина з інтернету. Вони можуть бути фішинговими. Наприклад, людина хоче отримати доступ до даних Вашого профілю чи іншої інформації.
10. Не переказуйте гроші людині, з якою спілкуєтеся на сайтах знайомств. На жаль, аферисти та аферистки можуть вигадувати різноманітні історії (навіть дуже зворушливі та жалісливі), щоб отримати від жертв кошти.
11. Не варто надсилати свої інтимні фото навіть тій людині, яка викликає у вас симпатію і не є схожою на зловмисника. Так Ви зможете уникнути шантажу і купи неприємностей у майбутньому.
12. Якщо Вам не хочеться спілкуватися, йти на побачення чи робити будь-які інші дії з людиною із сайту знайомств, не робіть цього. Не варто силувати та ламати себе. Прислухайтеся до себе і своїх відчуттів.

КОНТАКТИ ДЛЯ ДОПОМОГИ, ЯКЩО ВИ СТРАЖДАЄТЕ ВІД НАСИЛЬСТВА В ІНТЕРНЕТІ

Національна гаряча лінія для дітей та молоді – 0800500225 або 116111 (безкоштовно з усіх мобільних) чи в Telegram-chat – @CHL116111 або Instagram Direct – @childhotline_ua.

Поліція – 102.

Єдиний контакт-центр системи безоплатної правової допомоги – 0800213103.

Уповноважений Верховної Ради України з прав людини – 0800501720.

Сайт освітнього омбудсмена України – https://eo.gov.ua.

Кіберполіція – 0800505170.

Урядова консультаційна лінія з питань безпеки в інтернеті – 1545*3.

Бот про безпечну поведінку в інтернеті – @StopSextingBot.

Чатбот «Кіберпес» для боротьби з кібербулінгом (у Viber).

Чатбот «Кіберпес» для боротьби з кібербулінгом (у Telegram).

Корисні джерела для самонавчання:

Інформаційно-освітня кампанія #stop_sextинг.

1. Стаття «Кібербулінг – що це та як це зупинити?».
2. Наказ Міністерства освіти і науки України «Деякі питання реагування на випадки булінгу (цькування) та застосування заходів виховного впливу в закладах освіти» від 28.12.2019 № 1646.
3. Стаття «Кібербулінг та кібергрумінг: поняття, протидія, відповідальність».
4. Дія. Освіта. Кібербезпека.
5. Дія. Освіта. Освітній серіал «Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак».
6. DocuDaysUA. Кампанія проти кібербулінгу.

Навчальне видання

Синиціна Юлія Петрівна

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Методичні рекомендації для підготовки до практичних занять

(для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності D8 «Право»)

Редактор, оригінал-макет, дизайн –
А. В. Самотуга
Редактор *О. М. Врублевська*

Формат 60х84/16. Друк – цифровий. Гарнітура – Times New Roman.
Ум.-друк. арк. 3,20. Обл.-вид. арк. 3,44.

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до Державного реєстру видавців ДК № 8112 від 13.06.2024 р.