МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Конспект лекцій

(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 20.02.2025)

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 : конспект лекцій (для здобувачів другого (магістерського) рівня вищ. освіти зі спец. D8 «Право»). Дніпро : Дніпров. держ. ун-т внутр. справ, 2026. 62 с.

Конспект лекцій призначений для підготовки до лекційних занять із тем, що передбачені навчальним планом із дисципліни «Сучасні інформаційні технології в юридичній діяльності». Окрім теоретичного матеріалу, містить запитання для підсумкового контролю, словник термінів, а також список літератури.

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

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

ЗМІСТ

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: Атестаційна 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 матеріал для підготовки до лекційних 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

Лекція № 1 – 2 год.

Мета: ознайомити студентів з основними підходами до використання штучного інтелекту (далі – AI) у правозастосовній практиці, розкрити його можливості для автоматизації юридичної діяльності, розглянути потенційні ризики та етичні виклики, пов'язані зі впровадженням AI у сфері права, а також сформувати розуміння міжнародних стандартів та рекомендацій щодо безпечного та відповідального використання технологій.

План:

1. Вступ. Актуальність використання AI у правозастосуванні. Тенденції цифрової трансформації юридичної діяльності;
2. Поняття та напрями застосування штучного інтелекту у праві. Визначення штучного інтелекту. Основні сфери застосування: правосуддя, правнича аналітика, управління документами, криміналістика;
3. Інструменти AI для автоматизації юридичних досліджень. Огляд сучасних рішень: CaseLaw, ROSS Intelligence, ChatGPT та ін. Приклади використання в практиці юристів та судів;
4. Використання AI для прогнозування судових рішень. Методологія та приклади успішних проєктів. Обмеження та проблеми прогнозування (точність, контекст, правова невизначеність);
5. Юридичні ризики застосування AI. Загрози конфіденційності та захисту даних. Упередженість алгоритмів та ризик дискримінації. Проблема правового статусу рішень AI;
6. Етичні стандарти та рекомендації міжнародних організацій. Керівні принципи Ради Європи та Європейської комісії. Підхід ООН та ЮНЕСКО до регулювання AI. Національні стратегії у сфері етичного використання AI;
7. Висновки. Переваги та обмеження AI у праві. Необхідність балансу між інноваціями та безпекою.

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.

1. Вступ. Актуальність використання AI у правозастосуванні. Тенденції цифрової трансформації юридичної діяльності.

У сучасному світі правозастосовна практика зазнає суттєвих змін під впливом цифрових технологій. Одним із ключових напрямів цієї трансформації є впровадження систем штучного інтелекту (англ. artificial intelligence, AI), які вже сьогодні активно застосовуються у сфері права.

Актуальність використання AI у правозастосуванні зумовлена кількома чинниками:

– *зростанням обсягів інформації.* Юристи та суди щодня працюють із величезними масивами даних, судовими рішеннями, нормативно-правовими актами, що ускладнює оперативний аналіз останніх без застосування технологій;

– *необхідністю підвищення ефективності.* Автоматизація юридичних процесів дозволяє зменшити витрати часу та ресурсів, пришвидшити підготовку процесуальних документів і дослідження судової практики;

– *запитом на прозорість та доступність правосуддя.* AI може сприяти спрощенню доступу громадян до правової інформації та послуг.

Тенденціями цифрової трансформації юридичної діяльності є:

– автоматизація рутинних завдань – створення та перевірка документів, пошук прецедентів, підбір нормативних актів;

– використання прогнозної аналітики – системи, що здатна прогнозувати результати судових справ на основі попередніх рішень;

– розвиток електронного судочинства – створення онлайн-платформ для подання документів, проведення засідань у дистанційному режимі;

– інтеграція технологій OSINT та Big Data у правозастосуванні, що забезпечує швидкий пошук та обробку інформації з відкритих джерел;

– підвищення уваги до питань кібербезпеки та захисту персональних даних у зв’язку з використанням інтелектуальних систем.

Таким чином, впровадження штучного інтелекту у правову сферу є не лише технічною інновацією, а й необхідністю, продиктованою вимогами часу. Це відкриває широкі можливості для підвищення ефективності правосуддя, але водночас ставить перед суспільством нові виклики, пов’язані з безпекою, етикою та правовою відповідальністю.

2. Поняття та напрями застосування штучного інтелекту у праві. Визначення штучного інтелекту. Основні сфери застосування: правосуддя, правнича аналітика, управління документами, криміналістика.

Штучний інтелект – це сукупність технологій, що забезпечують здатність комп’ютерних систем виконувати завдання, що традиційно потребують людського інтелекту, як-от: аналіз інформації, розпізнавання образів, обробка природної мови, прогнозування та ухвалення рішень.

У праві AI розглядається як інструмент, що може підтримувати діяльність юристів, суддів та правоохоронних органів, підвищуючи ефективність і точність правозастосовної практики.

Основні напрями застосування AI у праві:

1. Правосуддя.

Автоматизовані системи аналізу судових рішень для пошуку аналогічних справ.

Прогнозування можливого результату справи на основі попередньої судової практики.

Підтримка суддів у підготовці проєктів рішень.

Електронне судочинство, що спрощує доступ громадян до правосуддя;

2. Правнича аналітика.

Використання AI для аналізу великих масивів правової інформації (законодавство, судова практика, міжнародні документи).

Автоматичне виявлення суперечностей у нормах права.

Прогнозна аналітика для оцінки юридичних ризиків у корпоративній діяльності;

3. Управління документами.

Автоматизація складання контрактів, процесуальних документів, угод.

Розпізнавання та структурування текстів із правовою інформацією.

Використання чат-ботів і віртуальних асистентів для надання базових юридичних консультацій;

4. Криміналістика та правоохоронна діяльність.

Аналіз цифрових доказів (листування, аудіо- та відеофайлів, логів).

Розпізнавання облич, відбитків пальців, голосу за допомогою біометричних технологій.

Використання OSINT-інструментів для збору доказової інформації з відкритих джерел.

Виявлення кіберзагроз, шахрайських схем та протиправної діяльності в інтернеті.

Таким чином, штучний інтелект у праві є багатофункціональним інструментом, що охоплює як аналітичні процеси, так і безпосереднє правозастосування. Його розвиток сприяє підвищенню ефективності правосуддя, проте потребує дотримання принципів законності, етики та захисту прав людини.

3. Інструменти AI для автоматизації юридичних досліджень. Огляд сучасних рішень: CaseLaw, ROSS Intelligence, ChatGPT та ін. Приклади використання в практиці юристів та судів.

Розвиток технологій штучного інтелекту привів до появи низки спеціалізованих платформ, що значно спрощують юридичні дослідження. Вони дозволяють швидко знаходити судові прецеденти, аналізувати великі обсяги нормативно-правових актів, формувати прогнози та рекомендації для

правозастосовної практики.

Огляд сучасних рішень:

1) CaseLaw Analytics.

Платформа для аналізу судової практики, що застосовує алгоритми AI для пошуку релевантних рішень.

Дозволяє визначати ймовірність успіху справи на основі аналізу прецедентів.

Використовується адвокатами та суддями у Франції, Німеччині та інших країнах ЄС для підвищення передбачуваності судових рішень;

2) ROSS Intelligence.

Юридична пошукова система, побудована на базі IBM Watson.

Дає змогу вводити запити природною мовою («чи може орендодавець розірвати договір без попередження?») та отримувати точні покликання на судові рішення та норми права.

Допомагає скоротити час на правові дослідження, що традиційно займали години або навіть дні.

3) ChatGPT та подібні LLM-моделі (Large Language Models).

Використовуються для генерації проєктів процесуальних документів, консультацій та узагальнення судової практики.

Можуть адаптувати текст під конкретний стиль юридичної мови, структурувати аргументи, створювати резюме рішень.

Наприклад, юристи застосовують ChatGPT для підготовки чорнових варіантів договорів, відповідей клієнтам або підсумків аналізу справ.

Інші інструменти.

LexisNexis та Westlaw – провідні бази правової інформації з елементами AI для розширеного пошуку та аналітики.

Luminance – платформа для автоматичного аналізу контрактів, що застосовується у сфері M&A.

Harvey AI – сучасний інструмент для юристів, інтегрований у роботу великих міжнародних юридичних фірм.

Приклади використання на практиці.

Юристи застосовують AI для швидкого пошуку прецедентів, аналізу законодавства, підготовки процесуальних документів та оцінки юридичних ризиків.

Суди у деяких країнах використовують аналітичні платформи для формування рекомендацій у типовій категорії справ (наприклад, щодо трудових спорів чи дорожніх правопорушень).

Адвокатські фірми інтегрують AI у внутрішні процеси, що дозволяє зменшити витрати часу на рутинну роботу і зосередитися на стратегічному захисті інтересів клієнтів.

Таким чином, сучасні інструменти AI суттєво змінюють підходи до юридичних досліджень, забезпечуючи швидкість, точність і зручність роботи з правовою інформацією. Водночас їх використання потребує критичного ставлення та перевірки результатів фахівцем-юристом.

4. Використання AI для прогнозування судових рішень. Методологія та приклади успішних проєктів. Обмеження та проблеми прогнозування (точність, контекст, правова невизначеність).

Одним із найбільш інноваційних напрямів застосування штучного інтелекту в праві є прогнозування результатів судових рішень. Використовуючи алгоритми машинного навчання та аналіз великих обсягів даних, системи AI можуть оцінювати ймовірність успіху тієї чи іншої позиції в суді.

Приклади застосування:

1) Європейський суд з прав людини (далі – ЄСПЛ).

Дослідники створили алгоритм, здатний із точністю майже 79 % передбачати рішення ЄСПЛ у справах, що стосуються порушень прав людини.

Модель аналізувала тексти скарг та попередні рішення, виявляючи закономірності у формуванні рішень;

2) США.

Платформи на кшталт Lex Machina та Premonition прогнозують поведінку суддів та адвокатів у конкретних категоріях справ.

Юристи використовують ці прогнози для вибору найбільш вигідної стратегії ведення справи;

3) Франція.

Декілька стартапів розробили інструменти аналізу судової практики з метою визначення ймовірності успіху у цивільних та адміністративних процесах.

Проте законодавство Франції обмежило подібну практику, заборонивши публічний аналіз рішень суддів для уникнення тиску на правосуддя;

4) Україна:

– система автоматичного розподілу судових справ. В українських судах діє система автоматизованого розподілу справ між суддями. Вона побудована на алгоритмах, що забезпечують рівномірне навантаження та виключають людський фактор при виборі судді;

– Єдиний державний реєстр судових рішень. Використовується для пошуку та аналітики судової практики.

Комерційні платформи (Liga360, YouControl, OpenDataBot) інтегрують елементи AI для швидкого пошуку рішень, виявлення закономірностей та прогнозування результатів.

YouControl.

Сервіс комплаєнс-аналітики, який застосовує алгоритми машинного навчання для виявлення ризиків, пов’язаних із контрагентами.

AI допомагає аналізувати судові справи, фінансові дані та репутаційні ризики компаній.

OpenDataBot.

Онлайн-платформа, що використовує алгоритми AI для моніторингу державних реєстрів (єдині державні реєстри, судові справи, податкові борги).

Дає змогу адвокатам та бізнесу отримувати сповіщення про нові судові процеси чи зміни в даних компаній.

ELSA Speak (українська адаптація в юридичній освіті).

Використовується в окремих закладах юридичної освіти як інструмент AI-асистента для навчання студентів пошуку правової інформації та аналізу кейсів.

Системи прогнозування банкрутства.

Українські фінансово-правові компанії тестують інструменти AI для прогнозування ймовірності банкрутства підприємств на основі відкритих фінансових і судових даних.

ChatGPT та подібні LLM-сервіси.

Використовуються юристами для первинної підготовки аналітичних довідок, складання шаблонів договорів, узагальнення судової практики.

Хоча офіційної інтеграції в державні органи поки немає, приватні юридичні фірми активно впроваджують ці рішення у свою діяльність.

Комерційні компанії.

Платформи штучного інтелекту аналізують тисячі рішень у справах про банкрутство, корпоративні конфлікти та інтелектуальну власність.

Це дозволяє компаніям приймати бізнес-рішення ще до початку судового процесу.

Обмеження та виклики.

Неповнота даних: алгоритми можуть працювати лише на основі наявних рішень, але не враховують унікальні обставини справи.

Упередженість алгоритмів: якщо дані містять системні упередження (наприклад, щодо певних соціальних груп), то AI лише відтворює їх і підсилює.

Правовий статус прогнозів: передбачення AI не можуть замінити незалежне рішення судді, вони є лише допоміжним інструментом.

Етичні аспекти: використання алгоритмів може створити ризик «автоматизованого правосуддя», що суперечить принципам справедливості.

Конфіденційність: великі масиви судових документів містять персональні дані, які можуть бути вразливими до витоків.

AI відкриває нові можливості для прогнозування результатів судових справ, проте він не здатен повністю замінити правозастосування людиною. Його роль полягає у підтримці юридичної діяльності, наданні додаткової інформації та підвищенні ефективності, але остаточне рішення завжди має залишатися за суддею.

5. Юридичні ризики застосування AI. Загрози конфіденційності та захисту даних. Упередженість алгоритмів та ризик дискримінації. Проблема правового статусу рішень AI.

Використання штучного інтелекту у правозастосуванні відкриває значні можливості, однак водночас створює низку юридичних ризиків, що потребують особливої уваги:

1) загрози конфіденційності та захисту даних.

AI-системи працюють із великими масивами персональних і чутливих даних. Обробка такої інформації може призвести до:

– несанкціонованого доступу та витоку персональних даних;

– порушення законодавства у сфері захисту приватності (наприклад, Закону України «Про захист персональних даних» або Регламенту (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR);

– використання даних без згоди суб'єкта.

Це створює серйозні ризики для прав людини та довіри до правосуддя;

2) упередженість алгоритмів та ризик дискримінації.

AI навчається на даних, що можуть містити приховані упередження (наприклад, щодо статі, віку, національності чи соціального статусу).

Унаслідок цього існує небезпека дискримінаційних рішень:

– прогнозування ризиків рецидиву у кримінальних справах може несправедливо обмежувати права певних груп;

– алгоритми правової аналітики можуть формувати викривлені висновки через некоректні чи неповні дані;

3) проблема правового статусу рішень AI.

Наразі відсутній чіткий правовий механізм визначення статусу рішень, ухвалених штучним інтелектом, у зв'язку з чим виникають запитання:

– чи може висновок AI вважатися доказом у суді;

– хто несе юридичну відповідальність у разі помилки алгоритму (розробник, користувач чи держава);

– чи є допустимим використання рішень AI для прогнозування судових результатів і чи не порушує це принципу незалежності суддів?

Отже, ключовими ризиками застосування AI у правозастосуванні є загроза приватності, можливість дискримінації та невизначений правовий статус алгоритмічних рішень. Подолання цих викликів потребує розвитку правової бази, етичних стандартів і контролю за використанням штучного інтелекту в юриспруденції.

6. Етичні стандарти та рекомендації міжнародних організацій. Керівні принципи Ради Європи та Європейської комісії. Підхід ООН та ЮНЕСКО до регулювання AI. Національні стратегії у сфері етичного використання AI.

Етичне регулювання застосування штучного інтелекту у правовій сфері є важливим чинником забезпечення довіри суспільства та дотримання прав людини. Міжнародні організації активно розробляють стандарти, спрямовані на безпечне та справедливе використання AI:

1) керівні принципи Ради Європи та Європейської комісії.

Рада Європи розробила: Європейську конвенцію з прав людини у

цифровому середовищі та рекомендації щодо застосування AI у сфері правосуддя. Основна ідея – AI не може замінити суддю, а лише допомагає йому в ухваленні рішень.

Європейська комісія представила Етичні настанови щодо надійного AI (Ethics Guidelines for Trustworthy AI), що ґрунтуються на таких принципах:

– повага до прав людини і верховенства права;
– прозорість алгоритмів та можливість перевірки їх роботи;
– недискримінаційність та справедливість;
– відповідальність за результати застосування AI.

Крім того, у 2024 р. ЄС ухвалив Регламент (ЄС) 2024/1689 Європейського парламенту і Ради, що встановлює гармонізовані правила щодо штучного інтелекту (Artificial Intelligence Act, AI Act) – перший у світі комплексний закон щодо штучного інтелекту, який встановлює класифікацію ризиків та вимоги до розробників;

2) підхід ООН та ЮНЕСКО до регулювання AI.

ООН підкреслює, що розвиток AI має відбуватися відповідно до Цілей сталого розвитку (Sustainable Development Goals, SDGs), зокрема для розширення доступу до правосуддя, боротьби з корупцією та нерівністю.

ЮНЕСКО у 2021 р. ухвалила Рекомендації щодо етики штучного інтелекту, де закріплено базові принципи, як-от:

– повага до людської гідності;
– заборона масового нагляду та маніпуляцій свідомістю;
– забезпечення цифрової безпеки та конфіденційності;
– підтримка культурної та соціальної різноманітності у використанні AI;

3) національні стратегії у сфері етичного використання AI.

Багато країн розробили власні стратегії розвитку та етичного регулювання AI.

Канада – стратегію «Responsible AI» з акцентом на прозорості урядових алгоритмів.

США – стратегію «AI Bill of Rights» (2022), що визначає права громадян на захист від дискримінації, доступність інформації про алгоритми та можливість оскарження рішень AI.

Україна – у 2020 р. схвалено Концепцію розвитку штучного інтелекту в Україні, що передбачає інтеграцію етичних норм у національне законодавство, розвиток прозорих стандартів та адаптацію до європейського AI Act.

7. Висновки. Переваги та обмеження AI у праві. Необхідність балансу між інноваціями та безпекою.

Таким чином, міжнародні організації та держави прагнуть сформувати єдині стандарти етичного використання AI, де ключовими залишаються права людини, прозорість, недискримінаційність та відповідальність. Для правозастосовної практики це означає, що будь-яке використання AI має проходити етичну та правову перевірку.

Застосування штучного інтелекту у правозастосовній практиці відкриває значні можливості для підвищення ефективності, доступності та прозорості юридичних процесів. AI допомагає юристам і суддям швидше опрацьовувати великі масиви правової інформації, прогнозувати можливі результати судових рішень, автоматизувати рутинні завдання, що зменшує витрати часу та ресурсів. Це сприяє більш якісному доступу громадян до правосуддя та зміцнює принцип верховенства права.

Водночас використання AI у праві має суттєві обмеження, пов'язані з такими ризиками, як: загрози порушення конфіденційності персональних даних; можливість упередженості алгоритмів, що може призвести до дискримінаційних рішень; проблема правового статусу рішень, ухвалених із залученням AI. Наявність цих ризиків потребує ретельного контролю, правового регулювання та етичної оцінки.

Ключовим завданням сучасного суспільства є пошук балансу між інноваціями та безпекою. З одного боку, необхідно підтримувати розвиток технологій, що сприяють ефективності правозастосування, а з іншого – створювати надійні механізми контролю, які гарантуватимуть дотримання прав людини, недопущення зловживань та забезпечення справедливості.

Отже, штучний інтелект у праві слід розглядати не як заміну людини, а як інструмент допомоги юристу і судді, який може підвищити якість правосуддя за умови належного етичного та правового регулювання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Чому використання штучного інтелекту у правозастосуванні вважається актуальним у сучасних умовах цифрової трансформації?
2. Сформулюйте визначення поняття «штучний інтелект» та поясніть його ключові характеристики.
3. Які основні напрями застосування штучного інтелекту у праві можна виокремити?
4. У чому полягає роль AI у сфері правосуддя та криміналістики?
5. Які сучасні інструменти штучного інтелекту застосовуються для автоматизації юридичних досліджень? Наведіть приклади.
6. Як інструменти CaseLaw, ROSS Intelligence, ChatGPT можуть використовуватися у практиці юристів і судів?
7. У чому полягають переваги і проблеми використання AI для прогнозування судових рішень?
8. Які основні юридичні ризики виникають при використанні штучного інтелекту у правозастосуванні?
9. Які етичні принципи та рекомендації щодо використання штучного інтелекту у праві були запропоновані Радою Європи, Європейською комісією, ООН та ЮНЕСКО?
10. Чим зумовлена необхідність пошуку балансу між інноваціями у сфері штучного інтелекту та безпекою правозастосовної діяльності?

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

Лекція № 2 – 2 год.

Мета: ознайомити студентів із поняттям, класифікацією та особливостями електронних доказів у кримінальному та цивільному процесах. Надати знання про правові вимоги та стандарти збору, збереження та подання цифрових доказів у суді. Розглянути основні методи фіксації, документування та забезпечення цілісності електронної інформації. Ознайомити з практичними методами та інструментами OSINT-технології для збору відкритої інформації. Розвинути навички критичного аналізу цифрових доказів та оцінки їх допустимості у судочинстві.

План:

1. Вступ. Актуальність цифрових доказів у сучасних кримінальних та цивільних процесах. Поняття електронної доказової бази;
2. Поняття та класифікація електронних доказів. Визначення цифрових доказів. Основні види електронних доказів: електронні листи, документи, аудіо/відеофайли, дані з соціальних мереж, журнали систем, хмарні дані тощо. Класифікація доказів за джерелом та форматом;
3. Правові вимоги до збору та подання цифрових доказів. Законодавче регулювання (Кримінальний процесуальний кодекс України, Цивільний процесуальний кодекс України, міжнародні стандарти). Дотримання принципів допустимості доказів. Питання конфіденційності та захисту персональних даних;
4. Методи фіксації та збереження електронної інформації. Технічні методи фіксації: знімки екранів, лог-файли, копії носіїв. Використання хешування для підтвердження цілісності даних. Документування процесу збору доказів. Забезпечення недоторканності та автентичності інформації;
5. Методи та інструменти OSINT-технологій. Поняття OSINT (Open Source Intelligence) та його роль у зборі цифрових доказів. Основні джерела інформації: соціальні мережі, публічні бази даних, вебсайти, форуми. Інструменти OSINT для збору, фільтрації та аналізу даних. Приклади практичного застосування OSINT у кримінальних та цивільних справах;
6. Висновки. Узагальнення ключових принципів збору та подання цифрових доказів.

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.

1. Вступ. Актуальність цифрових доказів у сучасних кримінальних та цивільних процесах. Поняття електронної доказової бази.

У сучасному світі більшість інформації створюється, обробляється та зберігається у цифровому вигляді. Це стосується як приватних, так і комерційних даних, а також інформації, що може стати доказом у правових спорах. З огляду на активне використання інформаційних технологій цифрові докази набувають все більшого значення у кримінальному та цивільному процесах.

Актуальність цифрових доказів зумовлена кількома ключовими чинниками, як-от:

– *зростання кількості кіберзлочинів* – шахрайство, хакерські атаки, незаконний доступ до інформації та інші правопорушення часто залишають цифровий слід, який є основним джерелом доказів;

– *поширення електронного документообігу та комунікацій* – електронні листи, чати, публікації у соціальних мережах та хмарні сервіси стають важливими джерелами інформації для встановлення фактів;

– *міжнародний характер багатьох справ* – цифрові дані легко передаються через кордони, що робить їх незамінними для розслідувань і цивільних спорів, пов’язаних із транскордонною діяльністю;

– *необхідність забезпечення достовірності та допустимості доказів* – для правового процесу важливо, щоб цифрові дані були зібрані та збережені відповідно до встановлених стандартів та процедур.

Поняття електронної доказової бази охоплює всі види інформації, що існує у цифровому форматі та може бути використана для підтвердження обставин справи в суді. *Електронна доказова база містить:*

– документи у цифровому вигляді (текстові файли, електронні договори, скановані копії);

– електронну кореспонденцію (електронні листи, повідомлення в месенджерах);

– аудіо- та відеозаписи;

– дані з інформаційних систем, журналів доступу, баз даних;

– публічну інформацію з інтернет-ресурсів та соціальних мереж, яку можна зафіксувати для судового розгляду.

Таким чином, цифрова доказова база є невід’ємною частиною сучасного правосуддя, оскільки дозволяє встановлювати факти, підтверджувати правопорушення та захищати законні права сторін у кримінальних та цивільних процесах.

2. Поняття та класифікація електронних доказів. Визначення цифрових доказів. Основні види електронних доказів: електронні листи, документи, аудіо/відеофайли, дані з соціальних мереж, журнали систем, хмарні дані тощо. Класифікація доказів за джерелом та форматом.

Цифрові або електронні докази – це будь-які дані, що існують у цифровому форматі та можуть бути використані для встановлення фактів у кримінальному чи цивільному процесі. Вони повинні мати ознаки достовірності, цілісності та допустимості, щоб бути прийнятими судом. Цифрові докази виникають у результаті використання комп'ютерних систем, інформаційних мереж, електронного документообігу, хмарних сервісів та комунікаційних платформ.

Основні види електронних доказів:

– *електронні листи та повідомлення у месенджерах* – підтверджують комунікацію між сторонами, домовленості або передачу інформації;

– *електронні документи* – договори, акти, заяви, скановані документи та інші файли, що мають юридичну силу;

– *аудіо- та відеозаписи* – записи розмов, конференцій, камер відеоспостереження, телефонних розмов;

– *дані з соціальних мереж та публічні інтернет-ресурси* – пости, коментарі, фото-, відеоматеріали, взаємодія користувачів;

– *журнали систем та лог-файли* – інформація про доступ до систем, операції користувачів, історію змін даних*;*

– *хмарні дані* – інформація, що зберігається на серверах провайдерів хмарних послуг (Google Drive, Dropbox, OneDrive тощо);

– *інші цифрові носії* – флеш-накопичувачі, жорсткі диски, мобільні пристрої, IoT-пристрої.

Класифікація цифрових доказів за джерелом та форматом наведена у таблиці 2.1.

Таблиця 2.1

Класифікація цифрових доказів за джерелом та форматом

№	Критерій класифікації	Приклади
1	За джерелом	Внутрішні дані організації (сервери, бази даних), зовнішні джерела (соціальні мережі, публічні ресурси), особисті пристрої учасників (смартфони, ноутбуки).
2	За форматом	Текстові файли, електронні таблиці, зображення, аудіо-, відеоматеріали, журнали систем, вебархіви, бази даних.
3	За способом отримання	Прямий доступ (знімки носіїв, копії систем), відкриті джерела (OSINT), дані від третіх осіб (провайдери послуг, свідки).

3. Правові вимоги до збору та подання цифрових доказів. Законодавче регулювання (Кримінальний процесуальний кодекс України, Цивільний процесуальний кодекс України, міжнародні стандарти). Дотримання принципів допустимості доказів. Питання конфіденційності та захисту персональних даних.

Правильна класифікація електронних доказів є важливою для визначення їхньої допустимості, надійності та методів їх збору, а також для вибору оптимальних технічних інструментів фіксації та аналізу інформації.

Цифрові докази, як і будь-які інші види доказів, мають збиратися та подаватися у суді відповідно до встановлених правових норм. Це необхідно для забезпечення допустимості, достовірності та об'єктивності доказової інформації.

Законодавче регулювання.

Кримінальний процесуальний кодекс України визначає порядок збору, фіксації та подання доказів у кримінальних провадженнях, включно з електронними, зокрема:

– право слідчих на вилучення цифрових носіїв та доступ до електронної інформації;

– порядок складання протоколів огляду цифрових пристроїв;

– правила збереження та захисту доказів для забезпечення їхньої цілісності.

Цивільний процесуальний кодекс України регламентує допустимість та оцінку доказів у цивільних справах. Цифрові докази можуть бути подані сторонами у вигляді електронних документів, записів комунікацій, даних з інформаційних систем або відкритих джерел.

Міжнародні стандарти (наприклад, резолюції ООН, стандарти ISO/IEC щодо електронної доказової бази) визначають універсальні вимоги до збереження цілісності цифрових даних, ведення журналів доступу та документування процесу збору доказів.

Дотримання принципів допустимості доказів.

Цифровий доказ вважається допустимим, якщо він зібраний у законний спосіб, не порушує права сторін та відповідає вимогам процесуальної достовірності.

Неправомірно отримані цифрові дані (наприклад, без дозволу власника або суду) можуть бути визнані недопустимими у суді.

Важливими критеріями допустимості є автентичність, цілісність та простежуваність доказу.

Питання конфіденційності та захисту персональних даних.

Збір цифрових доказів повинен враховувати вимоги законодавства про захист персональних даних (наприклад, Закону України «Про захист

персональних даних»).

Обробка електронної інформації не повинна порушувати права третіх осіб, що не є учасниками справи.

Забезпечується шифрування, контроль доступу та документування всіх дій зі збереження доказів, щоб уникнути витоку або маніпуляцій із даними.

Таким чином, правова рамка збору та подання цифрових доказів забезпечує баланс між ефективним розслідуванням та захистом законних прав та свобод учасників процесу.

4. Методи фіксації та збереження електронної інформації. Технічні методи фіксації: знімки екранів, лог-файли, копії носіїв. Використання хешування для підтвердження цілісності даних. Документування процесу збору доказів. Забезпечення недоторканності та автентичності інформації.

Електронні докази потребують особливих методів фіксації та збереження, щоб забезпечити їхню допустимість, достовірність і цілісність у судовому процесі. Неправильне збереження цифрових даних може призвести до втрати доказової сили або спростування їхньої достовірності.

Технічні методи фіксації електронної інформації.

Знімки екранів (screenshot) – швидкий спосіб зафіксувати поточний стан інформації на екрані комп'ютера або мобільного пристрою. Застосовується для використання як доказів переписок, вебсторінок, електронних документів.

Лог-файли та журнали систем – автоматично зберігають інформацію про операції користувачів, зміни файлів, дати та час доступу до систем. Дають змогу відновити хронологію подій.

Копії носіїв (forensic imaging) – створення побітових копій жорстких дисків, флеш-накопичувачів, карт пам'яті. Забезпечує можливість аналізу даних без ризику зміни оригінального носія.

Використання хешування для підтвердження цілісності даних.

Хеш-функції (MD5, SHA-256) дозволяють отримати унікальний цифровий підпис файлу або носія.

Будь-яка зміна даних змінює хеш, що дає змогу перевірити, чи не були дані підроблені або змінені після збору.

Документування процесу збору доказів.

Усі дії зі збору та фіксації електронної інформації повинні бути зафіксовані у протоколах або звітах.

У протоколах зазначаються: дата та час збору, опис носія, метод фіксації, дані про осіб, які брали участь, а також результати первинного аналізу.

Документування забезпечує простежуваність доказів і підтверджує, що вони були зібрані у законний спосіб.

Забезпечення недоторканності та автентичності інформації.

Використовуються методи фізичного та логічного захисту носіїв, шифрування, контроль доступу.

Забороняється необґрунтований доступ або модифікація даних сторонніми особами.

Дотримання цих правил гарантує, що цифрові докази зберігають свою юридичну цінність та можуть бути використані у суді.

Таким чином, системний підхід до фіксації та збереження електронної інформації є ключовим елементом забезпечення законності та ефективності використання цифрових доказів у кримінальних і цивільних процесах.

5. Методи та інструменти OSINT-технологій. Поняття OSINT (Open Source Intelligence) та його роль у зборі цифрових доказів. Основні джерела інформації: соціальні мережі, публічні бази даних, вебсайти, форуми. Інструменти OSINT для збору, фільтрації та аналізу даних. Приклади практичного застосування OSINT у кримінальних та цивільних справах.

OSINT (Open Source Intelligence) – це метод збору, аналізу та використання інформації з відкритих джерел. OSINT-технології дозволяють отримувати цінні дані для розслідувань, судових процесів та аналітики без порушення законодавства, використовуючи доступні публічні ресурси. У кримінальних та цивільних процесах OSINT допомагає:

– відстежувати факти та події, що мають значення для справи;
– підтверджувати або спростовувати заяви сторін;
– збирати інформацію про осіб, організації та їхню діяльність;
– формувати цифрову доказову базу на основі відкритих даних.

Основні джерела інформації для OSINT:

– соціальні мережі – Facebook, LinkedIn, Instagram, Telegram, Twitter; дозволяють отримувати публічні повідомлення, взаємодіяти користувачам, обмінюватися фото- та відеоматеріалами;

– публічні бази даних – реєстри компаній, судові рішення, державні портали, публічні статистичні ресурси;

– вебсайти та форуми – офіційні сайти організацій, тематичні форуми, блоги; дають змогу відстежувати заяви та діяльність суб’єктів;

– інші відкриті джерела – карти, геолокаційні сервіси, архіви, відкриті документи.

Інструменти OSINT для збору, фільтрації та аналізу даних:

– пошукові системи (Google, Bing) зі спеціальними операторами для глибокого пошуку;

– сервіси для моніторингу соціальних мереж та аналізу відкритих акаунтів;

– платформи для збору та обробки великих обсягів публічних даних (DataMiner, Maltego, SpiderFoot);

– інструменти перевірки автентичності медіафайлів та виявлення цифрових слідів (TinEye, FotoForensics).

Приклади практичного застосування OSINT у кримінальних та цивільних справах.

Виявлення шахрайських схем за допомогою перевірки активності в соціальних мережах та публічних реєстрах.

Підтвердження місцезнаходження особи за допомогою відкритих геолокаційних даних.

Збір доказів порушення авторських прав або неправомірного використання матеріалів шляхом аналізу вебсайтів та форумів.

Використання логів публічних платформ для встановлення хронології подій у цивільних спорах.

Таким чином, OSINT-технології є потужним інструментом для формування цифрової доказової бази, який доповнює традиційні методи збору електронних доказів і дозволяє підвищити ефективність кримінальних та цивільних розслідувань.

6. Висновки. Узагальнення ключових принципів збору та подання цифрових доказів.

У ході лекції було розглянуто ключові аспекти формування та використання цифрової доказової бази у кримінальних та цивільних процесах.

Отже:

– цифрові докази є невід’ємною частиною сучасного правосуддя. Вони дозволяють встановлювати факти, підтверджувати правопорушення та захищати права сторін у суді;

– правові вимоги до збору та подання цифрових доказів забезпечують їхню допустимість і достовірність. Важливими є законність збору, дотримання принципів конфіденційності та захист персональних даних;

– методи фіксації та збереження електронної інформації охоплюють технічні способи (знімки екранів, лог-файли, копії носіїв), хешування для перевірки цілісності даних та документування процесу збору доказів.

OSINT-технології дозволяють ефективно збирати, аналізувати та використовувати інформацію з відкритих джерел, доповнюючи традиційні методи збору цифрових доказів.

Ефективне використання цифрових доказів потребує поєднання правових знань, технічних навичок та аналітичного підходу. Застосування OSINT-технологій значно розширює можливості збору та перевірки інформації, підвищуючи ефективність розслідувань та якість судових рішень.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке цифрові або електронні докази і чим вони відрізняються від традиційних доказів у кримінальному та цивільному процесах?
2. Які чинники визначають актуальність використання цифрових доказів у сучасному правосудді?
3. Назвіть основні види електронних доказів і зробіть коротку характеристику кожного з них (електронні листи, документи, аудіо/відеофайли, дані з соціальних мереж, журнали систем, хмарні дані).
4. Як класифікують цифрові докази за джерелом і форматом? Наведіть приклади.
5. Які основні законодавчі акти регулюють збір і подання цифрових доказів у кримінальному та цивільному процесах України?
6. Що означає принцип допустимості цифрових доказів і які умови його дотримання?
7. Які вимоги щодо конфіденційності та захисту персональних даних необхідно враховувати при зборі електронних доказів?
8. Які технічні методи фіксації цифрових доказів застосовуються на практиці (знімки екранів, лог-файли, копії носіїв) і в чому полягають їхні особливості?
9. Як використовується хешування для підтвердження цілісності електронних доказів і чому це важливо для судового процесу?
10. Що таке OSINT, які основні джерела інформації він використовує і як OSINT-технології застосовуються у кримінальних та цивільних справах?

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

Лекція № 3 – 2 год.

Мета: ознайомити студентів із сучасними викликами та загрозами інформаційній безпеці у сфері юридичної діяльності. Розглянути стратегії захисту конфіденційної інформації від зовнішніх і внутрішніх загроз. Надати знання про сучасні технології та інструменти для захисту інформації, зокрема технічні та організаційні методи. Розвинути навички оцінки ризиків і планування комплексних заходів із кібербезпеки у юридичних організаціях. Ознайомити з принципами захисту персональних даних відповідно до законодавства та міжнародних стандартів.

План:

1. Вступ. Актуальність кібербезпеки у юридичній діяльності. Вплив цифровізації на управління юридичною інформацією;
2. Сучасні виклики та загрози інформаційній безпеці. Класифікація загроз: зовнішні (кіберзлочинність, хакерські атаки, фішинг) та внутрішні (помилки персоналу, несанкціонований доступ). Приклади реальних інцидентів у юридичних організаціях. Наслідки порушень інформаційної безпеки;
3. Стратегії захисту конфіденційної інформації. Превентивні стратегії: шифрування, багатофакторна аутентифікація, контроль доступу. Реактивні стратегії: моніторинг, виявлення вторгнень, резервне копіювання. Комплексний підхід до захисту даних у юридичних структурах;
4. Інноваційні технології та інструменти для захисту інформації. Антивірусні та антишпигунські програми. Системи виявлення та запобігання вторгненням (IDS/IPS). Хмарні сервіси безпеки, шифрування даних, цифрові сертифікати. Інструменти для моніторингу безпеки та аналізу ризиків;
5. Методи технічного захисту інформації. Шифрування даних, VPN, міжмережеві екрани (firewall). Контроль доступу на рівні систем та мереж. Резервне копіювання та відновлення даних;
6. Організаційні заходи інформаційної безпеки. Розробка та впровадження політик доступу та інструкцій для персоналу. Проведення аудиту безпеки та навчання працівників. Управління інцидентами та план реагування;
7. Захист персональних даних. Законодавчі вимоги щодо захисту персональних даних (Закон України «Про захист персональних даних», Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв’язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR). Методи

мінімізації ризиків витоку та неправомірного використання персональної інформації. Практичні поради щодо конфіденційності даних клієнтів та персоналу;

8. Основні висновки та рекомендації щодо забезпечення кібербезпеки юридичних даних.

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.

1. Вступ. Актуальність кібербезпеки у юридичній діяльності. Вплив цифровізації на управління юридичною інформацією.

Сучасна юридична діяльність неможлива без використання інформаційних технологій. Електронні документи, бази даних клієнтів, комунікації електронною поштою та спеціалізовані програмні системи роблять юридичну інформацію вразливою для різноманітних загроз.

Актуальність кібербезпеки зумовлена такими чинниками:

– зростання обсягів цифрової інформації – більшість документів і комунікацій зберігається в електронному вигляді, що підвищує ризик їх втрати або неправомірного використання;

– поширення кіберзлочинності – юридичні організації стають об'єктами кібератак, фішингу, шантажу або крадіжки даних;

– необхідність забезпечення конфіденційності та захисту персональних даних клієнтів і працівників – порушення захисту інформації може призвести до матеріальної та репутаційної шкоди;

– вимоги законодавства та стандартів – закони про захист персональних даних, стандарти ISO/IEC та інші нормативні документи встановлюють обов'язки щодо захисту інформації.

Ключова мета кібербезпеки у юридичній діяльності – забезпечити доступність, цілісність та конфіденційність інформації, що дозволяє захищати права клієнтів, підтримувати ефективність внутрішніх процесів і мінімізувати ризики виникнення інцидентів.

Таким чином, кібербезпека юридичних даних є невід'ємною складовою сучасного правового середовища, а знання методів та стратегій захисту інформації необхідне кожному фахівцю у сфері права.

2. Сучасні виклики та загрози інформаційній безпеці. Класифікація загроз: зовнішні (кіберзлочинність, хакерські атаки, фішинг) та внутрішні (помилки персоналу, несанкціонований доступ). Приклади реальних інцидентів у юридичних організаціях. Наслідки порушень інформаційної безпеки.

У сучасних юридичних організаціях інформаційна безпека є критично важливою, оскільки від стану захисту даних залежить конфіденційність клієнтів, ефективність процесів та репутація установи. Однак цифровізація створює нові виклики та загрози, що потребують системного підходу до їх виявлення та нейтралізації.

Класифікація загроз інформаційній безпеці:

1) зовнішні загрози – це небезпеки, що походять від третіх осіб або організацій, які намагаються отримати незаконний доступ до даних юридичної установи.

Основні види зовнішніх загроз:

– кіберзлочинність – крадіжка даних, шантаж (ransomware), фальсифікація документів, фінансові шахрайства тощо;

– хакерські атаки – цілеспрямовані спроби зламати інформаційні системи, отримати доступ до конфіденційних баз даних або порушити роботу серверів;

– фішинг – шахрайські спроби отримати доступ до паролів, електронних документів чи конфіденційної інформації за допомогою підроблених електронних листів або вебсайтів;

– шкідливе програмне забезпечення (malware, spyware, ransomware) – інфікування систем для крадіжки або блокування даних;

2) внутрішні загрози – це небезпеки, що походять зсередини організації.

Основні види:

– помилки персоналу – випадкова втрата даних, неправильне налаштування доступу або неправильне використання систем;

– несанкціонований доступ – дії співробітників, які перевищують свої повноваження або зловживають доступом до інформації;

– внутрішній саботаж – навмисне порушення роботи систем або викрадення даних для особистої вигоди.

Приклади реальних інцидентів у юридичних організаціях.

Кіберзлочинність: випадки витоку персональних даних клієнтів через ненадійні паролі або уразливі вебсайти юридичних фірм.

Фішинг: атаки на адвокатські контори за допомогою електронних листів, що імітують офіційні повідомлення банків або державних органів.

Внутрішні порушення: співробітники, які копіюють чи передають конфіденційні документи конкурентам або особисто використовують доступ до клієнтських баз даних.

Наслідки порушень інформаційної безпеки:

– фінансові збитки – витрати на відновлення даних, компенсації

клієнтам, штрафи та судові витрати;

– репутаційні втрати – втрата довіри клієнтів, партнерів та контролюючих органів;

– юридичні наслідки – притягнення до відповідальності за порушення законодавства про захист персональних даних або недотримання стандартів кібербезпеки;

– операційні ризики – збої у роботі систем, затримки у виконанні процесів, втрати важливих документів.

Сучасні юридичні організації стикаються з високим рівнем кіберзагроз, які потребують комплексного підходу до забезпечення інформаційної безпеки. Виявлення та класифікація загроз, навчання персоналу, впровадження технічних і організаційних заходів є ключовими складовими ефективного захисту даних.

3. Стратегії захисту конфіденційної інформації. Превентивні стратегії: шифрування, багатофакторна аутентифікація, контроль доступу. Реактивні стратегії: моніторинг, виявлення вторгнень, резервне копіювання. Комплексний підхід до захисту даних у юридичних структурах.

Захист конфіденційної інформації у юридичних організаціях вимагає застосування як превентивних, так і реактивних стратегій, а також комплексного підходу, що поєднує технічні, організаційні та процедурні заходи.

Превентивні стратегії. Превентивні заходи спрямовані на запобігання виникненню загроз та несанкціонованому доступу до інформації.

Основні методи:

1) шифрування даних.

Забезпечує конфіденційність інформації під час зберігання та передачі.

Використовуються симетричні (AES) та асиметричні (RSA) алгоритми шифрування.

Шифрування електронних листів, баз даних та документів захищає їх від сторонніх осіб у разі витоку;

2) багатофакторна аутентифікація (MFA).

Створює додаткові рівні захисту при вході до систем: пароль + одноразовий код (SMS, додаток аутентифікації) або біометричні дані.

Зменшує ризик несанкціонованого доступу навіть у разі компрометації пароля;

3) контроль доступу.

Встановлення паролів та прав доступу для співробітників згідно з їхніми обов’язками.

Забезпечує користувачам доступ тільки до ресурсів, необхідних для роботи.

Використання принципу «найменших привілеїв» зменшує ймовірність

внутрішніх загроз;

4) реактивні стратегії.

Реактивні заходи спрямовані на виявлення загроз та швидке реагування на інциденти з мінімізацією наслідків порушень;

5) моніторинг та виявлення вторгнень (IDS/IPS).

Системи контролюють мережевий трафік і активність користувачів для своєчасного виявлення підозрілих дій.

Можливість автоматичного блокування атак та сигналізація адміністраторам про інциденти;

6) резервне копіювання та відновлення даних.

Регулярне створення копій даних дозволяє відновити інформацію у разі втрати, пошкодження або шифрування зловмисниками (ransomware).

Використовуються як локальні, так і хмарні резервні копії для підвищення надійності;

7) аналіз інцидентів та навчання персоналу.

Вивчення попередніх порушень безпеки допомагає вдосконалювати процедури захисту.

Навчання співробітників методів безпечної роботи з даними знижує ризик внутрішніх загроз;

8) комплексний підхід до захисту даних у юридичних структурах.

Ефективна стратегія захисту інформації передбачає поєднання технічних, організаційних та процедурних заходів.

Технічні: шифрування, брандмауери, антивірус, багатофакторна аутентифікація.

Організаційні: політики доступу, аудит безпеки, навчання персоналу.

Процедурні: моніторинг, план реагування на інциденти, резервне копіювання.

Такий підхід дозволяє забезпечити конфіденційність, цілісність і доступність даних, що є критично важливим у юридичній діяльності, де інформація має високу цінність і потребує особливого захисту.

4. Інноваційні технології та інструменти для захисту інформації. Антивірусні та антишпигунські програми. Системи виявлення та запобігання вторгненням (IDS/IPS). Хмарні сервіси безпеки, шифрування даних, цифрові сертифікати. Інструменти для моніторингу безпеки та аналізу ризиків.

Сучасні юридичні організації активно використовують інноваційні технології для забезпечення інформаційної безпеки. Такі технології дозволяють ефективно захищати дані, автоматизувати процеси контролю доступу та мінімізувати ризики кіберзагроз.

Основні технології та інструменти захисту інформації:

1) антивірусні та антишпигунські програми.

Захищають комп’ютери та сервери від шкідливого програмного

забезпечення (malware, spyware, ransomware).

Регулярне оновлення баз даних вірусів дозволяє оперативно реагувати на нові загрози;

2) системи виявлення та запобігання вторгненням (IDS/IPS).

IDS (Intrusion Detection System) – система виявлення вторгнень, що контролює трафік і сигнали від мережевих пристроїв.

IPS (Intrusion Prevention System) – активна система, що не лише виявляє загрози, але й автоматично їх блокує;

3) хмарні сервіси безпеки та шифрування даних.

Хмарні сервіси використовуються для зберігання резервних копій та управління доступом до даних.

Шифрування хмарних файлів та переданих повідомлень забезпечує конфіденційність інформації;

4) цифрові сертифікати та електронний підпис.

Забезпечують автентичність документів та підтверджують їхню юридичну силу.

Електронні підписи та сертифікати дозволяють юридично фіксувати передачу даних між сторонами.

Інструменти для моніторингу безпеки та аналізу ризиків.

Програмні рішення для контролю подій у мережі, ведення логів і генерації звітів.

Інструменти аналізу ризиків дозволяють оцінювати ймовірність виникнення інцидентів та планувати превентивні заходи.

Приклади практичного застосування технологій.

Автоматизовані системи управління доступом у юридичних фірмах для контролю прав співробітників.

Антивірусні комплекси з централізованим моніторингом у державних юридичних установах.

Хмарні сервіси для зберігання договорів та архівних даних, що дозволяють відновлювати інформацію після інцидентів.

Системи IDS/IPS у корпоративних мережах для виявлення спроб несанкціонованого доступу.

Інноваційні технології та інструменти є невід'ємною частиною сучасної системи захисту юридичної інформації. Використання комплексних технічних рішень дозволяє забезпечити конфіденційність, цілісність та доступність даних, мінімізувати ризики кіберзагроз та підвищити ефективність управління інформаційною безпекою у юридичних структурах.

5. Методи технічного захисту інформації. Шифрування даних, VPN, міжмережеві екрани (firewall). Контроль доступу на рівні систем та мереж. Резервне копіювання та відновлення даних.

Технічний захист інформації є ключовим елементом кібербезпеки у юридичних організаціях. Він спрямований на запобігання несанкціонованому

доступу, захист даних від втрати або модифікації та забезпечення безперервності роботи систем.

Основні методи технічного захисту:

1) шифрування даних. Використовується для захисту інформації під час зберігання на носіях та передавання через мережі.

Симетричне шифрування (AES) – швидке шифрування великих обсягів даних.

Асиметричне шифрування (RSA) – забезпечує безпечний обмін ключами та автентифікацію учасників комунікації;

2) VPN (Virtual Private Network). Створює захищений канал зв'язку між користувачем та корпоративною мережею. Забезпечує конфіденційність даних при віддаленому доступі та роботу із внутрішніми ресурсами без ризику перехоплення інформації;

3) міжмережеві екрани (Firewall). Контролюють доступ до мережі та блокують небажаний або шкідливий трафік. Можуть фільтрувати дані за IP-адресами, портами, протоколами або типами додатків;

4) контроль доступу. Розмежування прав доступу користувачів відповідно до їхніх посадових обов'язків.

Впровадження принципу «мінімальних привілеїв» для зменшення ризику внутрішніх загроз;

5) резервне копіювання та відновлення даних. Регулярне створення резервних копій критично важливих даних. Застосування як локальних, так і хмарних копій для забезпечення відновлення після інцидентів, таких як атаки ransomware або випадкова втрата інформації;

6) системи виявлення та запобігання вторгнень (IDS/IPS):

– IDS – виявляє підозрілу активність у мережі та повідомляє адміністратора;

– IPS – не тільки виявляє загрози, але й автоматично блокує спроби вторгнення.

Методи технічного захисту інформації забезпечують безперервний контроль, захист від зовнішніх та внутрішніх загроз і підтримку цілісності юридичних даних. Їх застосування у поєднанні з організаційними та процедурними заходами формує надійну систему кібербезпеки, необхідну для сучасної юридичної діяльності.

6. Організаційні заходи інформаційної безпеки. Розробка та впровадження політик доступу та інструкцій для персоналу. Проведення аудиту безпеки та навчання працівників. Управління інцидентами та план реагування.

Організаційні заходи є невід'ємною частиною системи кібербезпеки у юридичних організаціях. Вони спрямовані на регламентування доступу, контроль дій персоналу і забезпечення виконання політик безпеки та доповнюють технічні методи захисту.

Основні організаційні заходи:

1) політики доступу та внутрішні правила безпеки. Розробка чітких політик доступу до інформаційних ресурсів відповідно до посадових обов'язків. Впровадження принципу «найменших привілеїв» – користувачі отримують лише ті права, що є необхідними для виконання їхніх завдань. Встановлення правил обробки, зберігання та передачі конфіденційної інформації;

2) аудит безпеки та моніторинг дій персоналу. Регулярне проведення внутрішніх аудитів безпеки для виявлення вразливостей. Контроль доступу до систем та документів, перевірка журналів дій користувачів. Виявлення потенційних загроз з боку співробітників та попередження внутрішніх порушень;

3) навчання та підвищення обізнаності персоналу. Проведення тренінгів із кібергігієни та правил безпечної роботи з інформацією. Ознайомлення співробітників із сучасними видами кібератак і методами їх уникнення. Формування культури безпеки в організації;

4) управління інцидентами та план реагування. Розробка планів дій на випадок інцидентів інформаційної безпеки (злом систем, витік даних, атаки шкідливого програмного забезпечення (далі – ПЗ)). Визначення ролей та відповідальності під час реагування на інциденти. Забезпечення оперативного відновлення функціонування систем і мінімізації наслідків.

Організаційні заходи дозволяють структуровано управляти ризиками та контролювати поведінку персоналу, що є критично важливим для захисту юридичних даних. Поєднання організаційних заходів із технічними та процедурними методами забезпечує комплексний підхід до інформаційної безпеки, мінімізуючи ймовірність втрат, витоку чи компрометації конфіденційної інформації.

6. Захист персональних даних. Законодавчі вимоги щодо захисту персональних даних (Закон України «Про захист персональних даних», Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR). Методи мінімізації ризиків витоку та неправомірного використання персональної інформації. Практичні поради щодо конфіденційності даних клієнтів та персоналу.

У юридичних організаціях захист персональних даних є критично важливим, оскільки інформація про клієнтів, співробітників та контрагентів має високу конфіденційність і цінність. Порушення цих даних може призвести до юридичної відповідальності, фінансових збитків та втрати довіри.

Основні принципи захисту персональних даних:

– *конфіденційність.* Дані повинні бути доступні лише уповноваженим особам. Використання шифрування, багатофакторної аутентифікації та

контроль доступу;

– *цілісність.* Забезпечення того, що дані не були змінені або пошкоджені сторонніми особами. Використання хешування, контрольних сум та логів змін інформації;

– *доступність.* Дані повинні бути доступні для законного використання у разі потреби. Резервне копіювання та відновлення інформації у разі інцидентів;

– *прозорість обробки даних.* Користувачі повинні бути поінформовані про те, які дані збираються, як вони зберігаються та обробляються. Дотримання принципів законодавства щодо персональних даних (Закон України «Про захист персональних даних», Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR).

Методи захисту персональних даних:

1) технічні методи.

Шифрування даних, контроль доступу, VPN, брандмауери.

Використання антивірусного та антимальварного програмного забезпечення;

2) організаційні методи.

Політики обробки персональних даних, інструкції для співробітників.

Навчання персоналу правилам безпечної роботи з конфіденційною інформацією;

3) процедурні заходи.

Ведення журналів доступу та змін даних.

План реагування на інциденти з персональними даними.

Аудит систем і перевірка дотримання законодавства.

Приклади практичного застосування.

Захист баз даних клієнтів адвокатських контор шляхом шифрування та багатофакторної аутентифікації.

Контроль доступу до конфіденційних справ тільки для співробітників, залучених до їх розгляду.

Використання хмарних сервісів із сертифікованим рівнем безпеки для зберігання архівних матеріалів.

Захист персональних даних у юридичних структурах є невід'ємною складовою інформаційної безпеки. Його ефективність досягається лише при поєднанні технічних, організаційних та процедурних методів, що дозволяє забезпечити конфіденційність, цілісність та доступність даних, а також відповідність законодавству.

8. Основні висновки та рекомендації щодо забезпечення кібербезпеки юридичних даних.

Сучасна юридична діяльність неможлива без ефективної системи кібербезпеки, оскільки цифрові дані є критично важливими для роботи організацій і потребують комплексного захисту.

Основні висновки:

– *цифровізація юридичної діяльності створює нові виклики.* Електронні документи, бази даних та комунікації цифровими каналами підвищують ризики витоку, модифікації або втрати інформації;

– *загрози інформаційній безпеці класифікуються на зовнішні та внутрішні.* Зовнішні: кіберзлочинність, хакерські атаки, фішинг, шкідливе програмне забезпечення. Внутрішні: помилки персоналу, несанкціонований доступ, саботаж;

– *ефективний захист інформації базується на поєднанні превентивних та реактивних стратегій.* Превентивні: шифрування, багатофакторна аутентифікація, контроль доступу. Реактивні: моніторинг, виявлення вторгнень, резервне копіювання, план реагування на інциденти;

– *інноваційні технології та інструменти забезпечують додатковий рівень безпеки* (антивірусні програми, IDS/IPS, хмарні сервіси, цифрові сертифікати та інструменти моніторингу ризиків);

– *організаційні заходи є критично важливими для контролю доступу та навчання персоналу* (політики безпеки, аудит систем, навчання працівників, ведення журналів доступу);

– *захист персональних даних є невід'ємною частиною кібербезпеки юридичних організацій* (дотримання принципів конфіденційності, цілісності та доступності даних відповідно до законодавства).

Рекомендації щодо забезпечення кібербезпеки:

– впроваджувати комплексну систему кібербезпеки, що поєднує технічні, організаційні та процедурні заходи;

– регулярно проводити аудит систем та моніторинг мережевої активності для виявлення потенційних загроз;

– використовувати сучасні інноваційні технології: шифрування, VPN, багатофакторну аутентифікацію, системи IDS/IPS;

– навчати персонал правильної обробки інформації та правил кібергігієни;

– забезпечувати захист персональних даних клієнтів і співробітників, дотримуючись законодавчих вимог і міжнародних стандартів.

Практичні приклади застосування.

Адвокатська контора впровадила шифрування електронної пошти та документів, а також багатофакторну аутентифікацію для всіх користувачів – випадків витоку інформації не зафіксовано протягом року.

Юридичний департамент державної установи налаштував IDS/IPS та регулярне резервне копіювання баз даних, що дозволило швидко відновити

інформацію після атак шкідливого ПЗ.

Корпоративна юридична служба розробила політику доступу і внутрішні правила роботи з клієнтськими даними, що скоротило внутрішні порушення доступу на 80 %.

Комплексний підхід до кібербезпеки юридичних даних, що поєднує технічні, організаційні та процедурні заходи, дозволяє мінімізувати ризики, забезпечити конфіденційність, цілісність та доступність інформації та підвищити ефективність роботи юридичних організацій у цифрову епоху.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке кібербезпека у юридичній діяльності і чому вона є актуальною в умовах цифровізації?
2. Які чинники визначають підвищений ризик для юридичної інформації у цифровому середовищі?
3. Назвіть основні зовнішні загрози інформаційній безпеці юридичних організацій.
4. Які внутрішні загрози можуть впливати на безпеку юридичних даних?
5. Які наслідки для юридичної організації може мати порушення інформаційної безпеки?
6. У чому полягають превентивні стратегії захисту конфіденційної інформації? Наведіть приклади їх застосування.
7. Які заходи належать до реактивних стратегій кібербезпеки і як вони мінімізують наслідки інцидентів?
8. Назвіть інноваційні технології та інструменти, що використовуються для захисту інформації у юридичних структурах.
9. Які основні технічні методи захисту інформації застосовуються для забезпечення конфіденційності, цілісності та доступності даних?
10. Які організаційні та законодавчі заходи слід впроваджувати для захисту персональних даних клієнтів і співробітників юридичних організацій?

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

Лекція № 4 – 2 год.

Мета: навчити студентів ефективно та безпечно здійснювати пошук правової інформації в мережі Інтернет, ознайомити з різними типами пошукових систем, спеціалізованими сервісами та інструментами OSINT, а також сформувати базові навички особистої безпеки в цифровому середовищі.

План:

1. Вступ. Актуальність пошуку правової інформації в інтернеті. Роль інформаційних технологій у юридичній діяльності;
2. Історія розвитку та загальна характеристика пошукових систем. Поява перших пошукових систем. Класифікація сучасних пошукових систем: загальні, спеціалізовані, метапошукові;
3. Пошук інформації за допомогою Google. Основні сервіси Google: пошук документів, зображень, карт, новин, академічні ресурси. Спеціальний пошук: оператори, фільтри, розширені опції. Інструменти для аналітики та апаратне забезпечення;
4. Метапошукові системи та системи анонімного пошуку інформації. Переваги та особливості метапошуку. Інструменти для анонімного пошуку: Tor, DuckDuckGo та ін.;
5. Пошук оперативної інформації в соціальних мережах. Використання Facebook для збору інформації. Методи аналізу публічних даних та профілів.
6. Застосування чат-ботів у месенджері Telegram. Використання ботів для пошуку, моніторингу та автоматизації збору даних. Практичні приклади застосування у правовій діяльності;
7. Особиста безпека в інтернеті. Основні принципи кібергігієни та захисту персональних даних. Виявлення фішингових атак, шкідливих сайтів та соціальної інженерії. Використання VPN, антивірусів, двофакторної аутентифікації;
8. Основні висновки щодо ефективного та безпечного пошуку правової інформації. Практичні поради щодо підвищення цифрової обізнаності та безпеки.

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.

1. Вступ. Актуальність пошуку правової інформації в інтернеті. Роль інформаційних технологій у юридичній діяльності.

Сучасна юридична практика неможлива без оперативного доступу до великого обсягу правової інформації. Інтернет став основним джерелом даних для адвокатів, юристів, нотаріусів та інших фахівців у правовій сфері, оскільки він дозволяє швидко знаходити законодавчі акти, приклади із судової практики, нормативні документи, аналітичні матеріали та коментарі експертів.

Актуальність пошуку правової інформації в інтернеті:

– *швидкий доступ до актуальної інформації*. Законодавство та судова практика постійно змінюються, і використання традиційних друкованих джерел не завжди дозволяє отримати оновлені дані. Інтернет забезпечує миттєвий доступ до текстів законів, постанов, рішень судів та нормативних документів;

– *економія часу та ресурсів.* Пошук онлайн скорочує час на збір та аналіз документів. Юридичні фахівці можуть швидко відслідковувати зміни у законодавстві та підготовлювати аналітичні матеріали;

– *можливість використання спеціалізованих ресурсів.* Правові бази даних, електронні бібліотеки, сервіси аналітики та метапошукові системи дозволяють ефективно працювати з великими обсягами інформації. Доступ до міжнародних нормативних актів та судової практики допомагає у підготовці міжнародних юридичних консультацій.

Роль інформаційних технологій у юридичній діяльності.

Автоматизація процесів. Використання програм для управління документацією, створення шаблонів договорів та ведення баз клієнтів зменшує людський фактор і підвищує ефективність роботи.

Аналітика та обробка великих обсягів даних. Технології AI та машинного навчання дозволяють аналізувати великі масиви судових рішень, виявляти тенденції та прогнозувати можливі юридичні ризики.

Підвищення доступності правової інформації. Онлайн-ресурси роблять законодавчі акти та судові рішення доступними не лише для професійних юристів, а й для громадян, що сприяє підвищенню правової обізнаності населення.

Інтеграція з іншими цифровими інструментами. Використання месенджерів, чат-ботів, систем OSINT та хмарних сервісів дозволяє збирати, аналізувати та систематизувати правову інформацію оперативно та безпечно.

Пошук правової інформації в інтернеті є невід’ємною частиною сучасної юридичної практики. Інформаційні технології значно підвищують ефективність роботи юристів, дозволяють оперативно отримувати, аналізувати та застосовувати дані, а також забезпечують безпечне та систематизоване ведення юридичної діяльності.

2. Історія розвитку та загальна характеристика пошукових систем. Поява перших пошукових систем. Класифікація сучасних пошукових систем: загальні, спеціалізовані, метапошукові.

Пошукові системи є основним інструментом для пошуку інформації в інтернеті. Вони дозволяють користувачам знаходити необхідні дані швидко та ефективно, сортувати їх за релевантністю та типом джерела, а також забезпечують доступ до великої кількості правових і аналітичних матеріалів.

Історія розвитку пошукових систем.

Перші пошукові системи. У 1990-х роках з'явилися перші пошукові системи, як-от Archie, Veronica та Lycos, які дозволяли знаходити файли на серверах FTP та вебсторінки. Вони мали обмежений функціонал і працювали переважно з текстовими файлами.

Розвиток вебпошуку. Поява Google у 1998 р. змінила підхід до пошуку: було впроваджено алгоритм ранжування PageRank, що враховував кількість та якість посилань на сторінку. З'явилися індексовані бази даних вебсторінок, що значно підвищило точність пошуку.

Сучасні пошукові системи. Крім Google, з'явилися Yahoo, Bing, Baidu та інші системи, що пропонують широкий спектр сервісів: новини, карти, зображення, відео, академічні джерела. Розвиток спеціалізованих та тематичних пошукових систем дозволив ефективно знаходити вузькоспеціалізовану інформацію, зокрема юридичну.

Загальна характеристика пошукових систем.

Типи пошукових систем:

1) загальні: Google, Bing, Yahoo – призначені для широкого кола користувачів та пошуку будь-якої інформації;

2) спеціалізовані: правові бази даних, наукові ресурси, державні портали.

3) метапошукові: агрегують результати з кількох джерел одночасно, підвищуючи точність пошуку.

4) анонімні: DuckDuckGo, Tor Search – забезпечують приватність користувачів під час пошуку.

Ключові функції сучасних пошукових систем:

– індексація вебсторінок та документів;

– використання алгоритмів ранжування для визначення релевантності результатів;

– підтримка спеціальних операторів для точного пошуку (наприклад, «» для точного збігу, site: для пошуку на конкретному сайті);

– інтеграція з додатковими сервісами: карти, календарі, перекладачі, хмарні сховища.

Переваги пошукових систем для юридичної діяльності:

– швидкий доступ до нормативно-правових актів, судової практики,

коментарів експертів;

– можливість використовувати фільтри та спеціальні опції для точного пошуку правової інформації;

– інтеграція з аналітичними інструментами для збору та обробки даних.

Сучасні пошукові системи є незамінним інструментом у юридичній діяльності. Вони дозволяють оперативно отримувати, систематизувати та аналізувати великі обсяги правової інформації, підвищують ефективність роботи фахівців та забезпечують швидкий доступ до необхідних даних для прийняття юридично обґрунтованих рішень.

3. Пошук інформації за допомогою Google. Основні сервіси Google: пошук документів, зображень, карт, новин, академічні ресурси. Спеціальний пошук: оператори, фільтри, розширені опції. Інструменти для аналітики та апаратне забезпечення.

Google є однією з найпопулярніших пошукових систем у світі та незамінним інструментом для збору юридичної інформації. Вона дозволяє швидко знаходити документи, судові рішення, нормативні акти, аналітичні матеріали та інші джерела.

Основні сервіси Google для пошуку інформації.

Google Search – основний сервіс для загального пошуку інформації.

Google Scholar – спеціалізований сервіс для пошуку наукових публікацій, включно з юридичними статтями та коментарями.

Google Books – доступ до електронних книг, зокрема юридичної літератури та монографій.

Google News – оперативний доступ до новинних матеріалів, зокрема правових новин та судових рішень.

Google Maps – використовується для перевірки адрес, локацій та організацій.

Google Drive – хмарне сховище для зберігання та спільного використання документів.

Спеціальний пошук у Google.

Використання операторів пошуку:

«» – пошук точного збігу фрази;

site: – пошук на конкретному сайті;

filetype: – пошук файлів певного формату (PDF, DOCX, XLS);

- – виключення слів із результатів пошуку.

Фільтри та інструменти.

Фільтри за датою, регіоном, типом контенту.

Використання розширених налаштувань для звуження результатів пошуку.

Апаратне забезпечення та інструменти Google для аналітики.

Google Analytics – аналіз вебтрафіку та поведінки користувачів на сайтах.

Google Alerts – налаштування сповіщень про нові публікації за ключовими словами, що дозволяє відслідковувати зміни в законодавстві або нові судові рішення.

Google Cloud Platform – хмарні ресурси для обробки великих обсягів інформації та аналітики.

Переваги використання Google у юридичній діяльності:

– швидкий доступ до актуальної правової інформації;
– можливість точного пошуку за допомогою спеціальних операторів;
– інтеграція з іншими сервісами для зручного зберігання, обробки та аналізу даних;
– автоматичне сповіщення про зміни у законодавстві та нові публікації.

Google є потужним інструментом для збору юридичної інформації, що дозволяє фахівцям швидко знаходити необхідні документи, аналізувати їх і підтримувати актуальність знань. Використання спеціального пошуку, додаткових сервісів та аналітичних інструментів підвищує ефективність роботи юристів та полегшує процес прийняття рішень.

4. Метапошукові системи та системи анонімного пошуку інформації. Переваги та особливості метапошуку. Інструменти для анонімного пошуку: Tor, DuckDuckGo та ін.

У сучасній практиці пошуку інформації важливу роль відіграють метапошукові системи та системи анонімного пошуку, які забезпечують ефективне агрегування даних і підвищують конфіденційність користувача.

Метапошукові системи.

Метапошукові системи не зберігають власного індексу сторінок, а збирають результати одночасно з кількох пошукових систем.

Вони надають користувачу узагальнений список релевантних результатів із різних джерел.

Переваги використання. Ширше охоплення інформації, ніж при використанні однієї пошукової системи. Можливість швидко порівнювати результати з різних платформ. Підвищення точності пошуку за рахунок агрегування результатів.

Приклади метапошукових систем: Dogpile, Metacrawler, Yippy.

Вони дозволяють одночасно шукати в Google, Bing, Yahoo та інших джерелах.

Системи анонімного пошуку інформації.

Системи анонімного пошуку забезпечують конфіденційність

користувача, не зберігаючи персональні дані та історію запитів. Використовують проксі-сервери, шифрування та технології приховування IP-адреси.

Переваги використання. Захист особистих даних та запобігання відстеженню дій користувача. Можливість отримати результати пошуку без персоналізації та комерційного фільтрування. Підвищена безпека при роботі з чутливою інформацією.

Приклади систем анонімного пошуку.

DuckDuckGo – пошукова система, що не відслідковує запити користувача.

Startpage – агрегує результати Google, не зберігаючи персональні дані.

Tor Search – доступ через мережу Tor для анонімного пошуку інформації.

Метапошукові системи та системи анонімного пошуку забезпечують розширені можливості збору інформації та захист конфіденційності користувача. Вони є особливо корисними для юридичних фахівців, які працюють із великим обсягом публічних даних, оперативною інформацією та чутливими матеріалами.

5. Пошук оперативної інформації в соціальних мережах. Використання Facebook для збору інформації. Методи аналізу публічних даних та профілів.

Соціальні мережі стали важливим джерелом оперативної інформації для юридичних фахівців. Вони дозволяють отримувати актуальні дані про осіб, організації, події та громадські настрої, що може бути корисним у підготовці юридичних справ, аналітичних матеріалів або правової оцінки ситуацій.

Соціальні мережі як джерело інформації.

Facebook – найпопулярніша соціальна мережа, де користувачі публікують особисту, професійну та суспільну інформацію. Крім того, вона надає можливість відслідковувати події, офіційні сторінки організацій, групи за інтересами та публічні пости.

Методи пошуку інформації в соціальних мережах.

Використання вбудованих пошукових функцій для знаходження користувачів, груп і постів. Використання фільтрів за датою, географією, типом публікації. Аналіз публічних даних профілів для отримання інформації про зв’язки, активність та інтереси.

Інструменти OSINT для соціальних мереж.

Сервіси для збору, агрегування та аналізу публічних даних (наприклад, Maltego, Social Blade, Pipl).

Використання ботів та скриптів для автоматичного збору інформації з

відкритих джерел.

Правові та етичні аспекти.

Збір даних повинен здійснюватися з дотриманням законодавства та принципів конфіденційності.

Необхідно відрізняти публічну інформацію, доступну для аналізу, від приватних даних користувачів.

Юридичні фахівці мають дотримуватися етичних норм та правил професійної діяльності, щоб уникнути порушень прав користувачів.

Практичні поради:

1) використовувати публічні профілі та сторінки організацій для збору даних;

2) налаштовувати сповіщення про нові публікації у групах або на сторінках, що цікавлять;

3) застосовувати OSINT-інструменти для систематизації та аналізу отриманої інформації;

4) зберігати отримані дані з документуванням джерел для подальшого використання у правовій діяльності.

Соціальні мережі є цінним джерелом оперативної інформації для юридичних фахівців. Їх ефективне використання можливе лише за умови поєднання технічних інструментів збору даних, аналітичних методик та дотримання правових і етичних стандартів.

6. Застосування чат-ботів у месенджері Telegram. Використання ботів для пошуку, моніторингу та автоматизації збору даних. Практичні приклади застосування у правовій діяльності.

Чат-боти в месенджері Telegram стали ефективним інструментом для збору, автоматизації та аналізу інформації, у тому числі в юридичній діяльності. Вони дозволяють отримувати оперативні дані, моніторити події та взаємодіяти з великою кількістю джерел у режимі реального часу.

Основні можливості чат-ботів у Telegram:

– *автоматичний збір інформації.* Чат-боти можуть регулярно відстежувати публікації у групах, каналах та окремих акаунтах. Дозволяють збирати контактні дані, публікації, новини або статистичні показники;

– *моніторинг і аналітика.* Боти можуть аналізувати тенденції, популярні теми та активність користувачів. Використовуються для швидкого відстеження змін у законодавстві, рішень у судових справах або правових новин;

– *автоматизація рутинних завдань* (надсилання сповіщень про нові публікації або події; підготовка звітів та узагальнень інформації; використання шаблонів для швидкого збору даних із декількох джерел одночасно).

Приклади практичного застосування у юридичній діяльності.

Моніторинг нових публікацій у тематичних каналах, що стосуються змін

законодавства.

Автоматичне отримання аналітичних матеріалів або пресрелізів від органів влади.

Збір відкритих даних про контрагентів або сторін судових справ із публічних джерел для правової оцінки.

Рекомендації щодо безпечного використання:

1) використовувати офіційні або перевірені боти, щоб уникнути шкідливого ПЗ;

2) дотримуватися законодавства про персональні дані та не збирати конфіденційну інформацію без дозволу;

3) зберігати отримані дані у структурованому вигляді з документуванням джерел для подальшого використання;

4) обмежувати доступ до ботів лише уповноваженим працівникам.

Чат-боти Telegram забезпечують оперативний і автоматизований доступ до великого обсягу інформації, підвищують ефективність роботи юридичних фахівців та дозволяють швидко реагувати на зміни в законодавстві та суспільному середовищі. Їх використання має поєднуватися з дотриманням правових та етичних стандартів.

7. Особиста безпека в інтернеті. Основні принципи кібергігієни та захисту персональних даних. Виявлення фішингових атак, шкідливих сайтів та соціальної інженерії. Використання VPN, антивірусів, двофакторної аутентифікації.

Особиста безпека в інтернеті є критично важливою для юридичних фахівців, оскільки робота з правовою інформацією часто передбачає обробку конфіденційних даних клієнтів, державних та корпоративних структур. Недотримання базових принципів кібергігієни може призвести до витоку інформації, кібератак та репутаційних втрат.

Основні принципи особистої безпеки в інтернеті:

1) захист персональних даних. Використання надійних паролів та двофакторної аутентифікації (2FA). Обмеження розкриття особистої інформації в соцмережах та професійних профілях;

2) використання безпечних каналів зв'язку. Застосування VPN для захисту трафіку при підключенні до публічних мереж. Шифрування електронних листів та документів для забезпечення конфіденційності;

3) розпізнавання та уникнення загроз. Виявлення фішингових листів, підозрілих посилань та шкідливих файлів. Регулярне оновлення антивірусного програмного забезпечення та системних патчів;

4) контроль доступу та безпечне зберігання інформації. Обмеження доступу до робочих пристроїв та баз даних. Використання резервного копіювання важливої інформації та захищених хмарних сховищ;

5) цифрова гігієна та поведінка в мережі. Забезпечення відсутності публікації конфіденційної інформації на відкритих платформах. Використання офіційних та перевірених сервісів для роботи з документами та комунікації.

Практичні поради:

– регулярно змінювати паролі та не використовувати однакові для різних сервісів;

– використовувати менеджери паролів для зберігання складних комбінацій;

– активувати сповіщення про підозрілу активність у профілях та акаунтах;

– навчати персонал основ кібергігієни та правил безпечного поводження з інформацією.

Дотримання правил особистої безпеки в інтернеті є необхідною умовою для ефективної та безпечної роботи юриста. Це дозволяє захистити конфіденційну інформацію, зменшити ризик кібератак і забезпечити відповідність законодавчим та етичним стандартам при роботі з цифровими джерелами інформації.

8. Основні висновки щодо ефективного та безпечного пошуку правової інформації. Практичні поради щодо підвищення цифрової обізнаності та безпеки.

Пошук правової інформації в інтернеті є ключовим елементом сучасної юридичної практики. Ефективність і безпека цього процесу залежать від поєднання правильних інструментів, методик пошуку та дотримання правил кібергігієни.

Основні висновки:

1) *розвиток пошукових систем значно полегшив доступ до правової інформації.* Використання Google та спеціалізованих правових баз даних забезпечує швидкий доступ до нормативних актів, судової практики та аналітичних матеріалів;

2) *метапошукові та анонімні системи підвищують ефективність та безпеку пошуку.* Вони дозволяють одночасно шукати інформацію з кількох джерел та захищають особисті дані користувача;

3) *соціальні мережі та месенджери є важливими джерелами оперативної інформації.* Facebook і Telegram (за допомогою чат-ботів) дозволяють збирати актуальні дані, але при цьому потрібно дотримуватися правових та етичних норм;

4) *особиста безпека в інтернеті є критичною складовою професійної діяльності юриста.* Захист паролів, двофакторна аутентифікація, VPN, шифрування та цифрова гігієна зменшують ризики витоку конфіденційної інформації.

Рекомендації:

1) використовувати комбінацію різних інструментів пошуку (Google, метапошукові системи, спеціалізовані правові бази даних та соціальні мережі);

2) застосовувати спеціальні оператори та фільтри для точного пошуку нормативних актів, судових рішень та аналітичних матеріалів;

3) документувати джерела інформації;

4) зберігати покликання, дати доступу та опис отриманих даних для подальшого використання у правових процедурах;

5) дотримуватися правил безпеки та конфіденційності;

6) використовувати надійні паролі, антивірусні програми, VPN та шифрування;

7) уникати розкриття конфіденційної інформації у відкритих джерелах;

8) навчати та інструктувати персонал. Працівники юридичних організацій повинні знати основи пошуку інформації та правила безпечної роботи в інтернеті.

Ефективний і безпечний пошук правової інформації в інтернеті є необхідною компетенцією сучасного юриста. Поєднання технічних навичок, знання інструментів пошуку та дотримання правил кібергігієни дозволяє забезпечити достовірність даних, оперативність доступу до інформації та захист конфіденційної інформації клієнтів і організацій.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Наскільки актуальним є пошук правової інформації в інтернеті для сучасної юридичної діяльності та яку роль відіграють інформаційні технології?
2. Назвіть перші пошукові системи і коротко охарактеризуйте їхній функціонал.
3. Як класифікуються сучасні пошукові системи? Наведіть приклади загальних, спеціалізованих та метапошукових систем.
4. Які основні сервіси Google використовуються для пошуку правової інформації та які функції вони мають (пошук документів, зображень, карт, новин, академічні ресурси)?
5. Поясніть принцип використання операторів і фільтрів у спеціальному пошуку Google. Наведіть приклад їх застосування.
6. Що таке метапошукові системи та які переваги їх використання, як порівняти з окремими пошуковими системами?
7. Назвіть інструменти анонімного пошуку інформації та поясніть їхнє значення для безпечного збору даних.
8. Як використовуються соціальні мережі, зокрема Facebook, для пошуку оперативної правової інформації? Які методи аналізу публічних даних застосовуються?
9. Які можливості надають чат-боти у месенджері Telegram для збору та аналізу інформації у правовій діяльності? Наведіть приклад практичного застосування.
10. Назвіть основні принципи особистої безпеки в інтернеті для юридичних фахівців. Які заходи допомагають захистити персональні дані та уникнути кіберзагроз?

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, 9804 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.

ДЛЯ ДЕННОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота/ Індивідуальна робота	Залік (З) / ЕКЗАМЕН (Е)
≤ 40	≤ 10	
≤ 50		≤ 50
Підсумкова оцінка у випадку заліку (П) ПК + З ≤ 100		
Підсумкова оцінка у випадку складання екзамену (П) ПК + Е ≤ 100		

ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота/ Індивідуальна робота	Залік (З) / ЕКЗАМЕН (Е)
≤ 20	≤ 30	
≤ 50		≤ 50
Підсумкова оцінка у випадку заліку (П) ПК + З ≤ 100		
Підсумкова оцінка у випадку складання екзамену (П) ПК + Е ≤ 100		

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:

П ПК+З≤100,

де ПК – бали за поточний контроль (34–50 балів),
З – бали за результатами складання заліку.

Критерії оцінювання аудиторної роботи здобувачів вищої освіти (денної та заочної форм 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
(денна та заочна форми 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 – 10 (30) балів:

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) – 10 (30) балів;
2. Підготовка презентацій-доповідей для участі в роботі наукового студентського гуртка кафедри (надати презентацію та фото виступу) – 10 (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 – 10 (30) балів;
4. Отримання сертифікату після проходження онлайн-тесту «Цифроґрам 1.0 для громадян» на платформі «Дія.Освіта» https://osvita.diia.gov.ua/digigram – 10 (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» – 10 (30) балів;
6. Проходження тесту з самостійної роботи – 10 (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	Не зараховано	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.

Навчальне видання

Синиціна Юлія Петрівна

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Конспект лекцій

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

Редактор, оригінал-макет, дизайн –
А. В. Самотуга

Редактор *О. М. Врублевська*

Формат 60x84/16. Друк – цифровий. Гарнітура – Times New Roman.
Ум.-друк. арк. 3,35. Обл.-вид. арк. 3,75.

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