ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ЗАТВЕРДЖЕНО
Рішення методичної ради університету
29 серпня 2024 року,
протокол № 1.

Перша проректорка, голова методичної ради університету, кандидатка наук з державного управління, доцентка

_____ Ірина КОВТУН

29 серпня 2021 року

м.п.

НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ
навчальної дисципліни
«ІНФОРМАЦІЙНО_КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВНИЧІЙ ДІЯЛЬНОСТІ»
для підготовки на першому освітньому рівні здобувачів вищої освіти ступеня бакалавра
зі спеціальності 081 право
галузі знань 08 право
за денною формою навчання

м. Хмельницький
2024

РОЗРОБНИК:

доцентка кафедри, кандидатка педагогічних наук, доцентка _____ Ольга ФЕДОРЧУК
26 серпня 2024 року

СХВАЛЕНО

Рішення кафедри менеджменту, економіки, статистики та цифрових технологій
27 серпня 2024 року, протокол № 1.

Завідувачка кафедри,
кандидатка економічних наук, доцентка _____ Наталія ЗАХАРКЕВИЧ
26 серпня 2024 року

ПОГОДЖЕНО

Декан юридичного факультету, доцент _____ Віктор ЗАХАРЧУК
26 серпня 2024 року

Обліковий обсяг 2,8 ум.др.арк.

ЗМІСТ

1. Структура вивчення навчальної дисципліни

1.1. Тематичний план навчальної дисципліни

№ теми	Назва теми	Кількість годин											
		Денна форма навчання						Заочна форма навчання					
		Усього	у тому числі					Усього	у тому числі				
			Лекції	практичних	Лабор.	Ін.зав.	СРС		Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС
1	2	3		5	6	7	8	9	10	11	12	13	14
1.	Вступ до інформаційно-комунікаційних технологій у праві	4		-	–	2	2						
2.	Робота з даними у юридичній практиці	8		2	–	–	6						
3.	Складання та перевірка електронних договорів	10		4	–	–	6						
4.	Організація та налаштування електронного документообігу для юридичної фірми	10		4	–	–	6						
5.	CRM система і її роль в управлінні клієнтами та справами в юридичному бізнесі	12		6	–	–	6						
6.	Кіберзлочинність та правове регулювання	10		4	–	2	4						
7.	Електронне судочинство	16		8			8						
8	Цифрові інструменти в юридичній практиці	12		6			6						
9.	Мультимедійна підтримка юридичної діяльності	8		4			4						
	Всього годин:	**90**		**38**	**–**	**4**	**48**						

1.2. Практичні заняття

У матеріалах до практичних занять містяться питання для обговорення на навчальному занятті, завдання, наводяться переліки літератури і нормативно-правових актів, необхідних для вивчення теми заняття.

На заняттях застосовуються:

1) пошук інформації за індивідуальним завдання;

2) вирішення ситуаційних завдань;

3) кейсовий метод;

4) практичне використання інформаційних ресурсів.

Поточний контроль знань студентів з навчальної дисципліни може проводитися у формах:

1) усне або письмове (у тому числі тестове) бліц-опитування студентів щодо засвоєння матеріалу попередньої лекції;

2) усне або письмове (у тому числі тестове) опитування на семінарських заняттях;

3) презентація, аналітичні та статистичні звіти.

У матеріалах до занять також містяться питання для обговорення. У списку літератури зазначені роботи, знання яких необхідно студентам для засвоєння матеріалів теми і рішення задач; спеціальна література призначена для більш глибокого вивчення питань теми.

Таким чином, готуючись до занять по темі, треба:

уважно ознайомитися з планом заняття і списком нормативних актів, що рекомендуються, та навчальної та спеціальної літератури;

опрацювати нормативні акти з відповідної теми;

використовуючи вивчений матеріал, вирішити ситуаційні завдання та виконати практичні заняття, визначені навчально-методичними матеріалами, силабусом.

Усі питання, які виникають у студентів при підготовці до практичних занять, під час самостійної роботи, можуть бути вирішені під час групових та індивідуальних консультацій, що здійснюються викладачем, відповідно до затвердженого графіку.

Тема 2. Робота з даними у юридичній практиці

Практична робота № 1

Тема. Створення політики конфіденційності для юридичних фірм або комерційних проектів.

Мета. Ознайомити студентів з поняттям та значенням політики конфіденційності. Сформувати практичні аспекти забезпечення захисту персональних даних у цифровому середовищі згідно з GDPR та українським законодавством.

Завдання.

1. Визначити ключові аспекти конфіденційності:
   - Що таке політика конфіденційності та її призначення.
   - Основні вимоги до політик згідно з українським законодавством та GDPR.
   - Основні ризики витоку даних у юридичній практиці.
2. Підготувати огляд основних компонентів політики конфіденційності:
   - Які дані збираються (персональні, фінансові, контактні тощо).
   - Як обробляються та зберігаються дані.
   - Права користувачів щодо їхніх персональних даних.
   - Заходи безпеки для захисту інформації.
3. Підготувати структуру документа, що містить наступні розділи:
   - Вступ (мета політики, обсяг дії).
   - Перелік персональних даних, які збираються (ПІБ, IP-адреса, контактні дані).

- Мета обробки даних.
- Порядок передачі третім особам.
- Термін зберігання персональних даних.
- Права клієнтів та співробітників відповідно до законодавства.
- Контактні дані відповідальної особи (DPO - Data Protection Officer).

4. Створити документ політики конфіденційності для фіктивної юридичної фірми з урахуванням вимог GDPR та Закону України «Про захист персональних даних».

Файл зберегти під іменем ***Власне прізвище_1*** та розмістити у Класрумі

Тема 3. Складання та перевірка електронних договорів

Практична робота №2

Тема. Цифрова трансформація юридичної фірми «LexTech»

Передісторія кейсу:

Вступ. Юридична фірма «LexTech», яка спеціалізується на консультуванні корпоративних клієнтів і супроводі судових справ, зіткнулася з кількома проблемами в своїй діяльності. Основними викликами є:

1. **Низька ефективність документообігу**: більшість документів обробляється вручну, що спричиняє помилки, втрату часу та складнощі у відстеженні змін.
2. **Відсутність інтегрованої системи управління клієнтами**: записи про клієнтів та їхні справи ведуться в розрізнених файлах, що ускладнює доступ до актуальної інформації.
3. **Недостатня кібербезпека**: фірма використовує застарілі методи захисту даних, що становить ризик витоку конфіденційної інформації.
4. **Відсутність можливості працювати з електронним судом**: у співробітників недостатньо знань та інструментів для ефективної подачі документів в електронному вигляді.
5. **Невикористання сучасних технологій автоматизації**: підготовка документів, аналіз правових даних і комунікація виконуються без використання інноваційних цифрових рішень.

Фірма прагне вирішити ці проблеми, впровадивши комплексну цифрову трансформацію.

Мета. Розробити проект, який дозволить вирішити ці виклики за допомогою сучасних інформаційних технологій, інтегруючи інструменти автоматизації, управління даними та кібербезпеки.

Завдання.

1. На гугл диску в розділі **Мій диск** створити папку з назвою «**ІКТ-власне прізвище**» та створити структуру для збереження інформації, отриманої при виконанні практичних завдань курсу. Кількість вкладених папок рекомендується створити відповідно до кількості тем курсу. (див. Робочу програму).
2. Зберегти на диску власний ЕЦП для підписання документів.
3. Для роботи над груповими кейсами розподілити ***ролі та завдання***. Інформацію розмістити в таблиці.
4. Послідовність виконання практичної роботи (скріншоти з екрана та коментарі) подати у вигляді презентації. Зберегти з іменем ***Власне прізвище_2*** та розмістити у класрумі.
5. Організувати дозвіл членам групи для редагування інформації. Викладачу – для перегляду. Інформація про корпоративні акаунти студентів групи додається.

Практична робота №3-4

Тема. Створення пакета первинних документів для переддоговірних стосунків

Мета. Навчитися використовувати шаблони документів, розміщених у вільному доступі у мережі Інтернет та готувати їх для подальшого використання у СЕД.

.Завантажити довідково-інформаційну платформу правових консультацій WikiLegalAid за посиланням https://wiki.legalaid.gov.ua/

1. За необхідності зареєструватися на платформі.
2. Ознайомитися з принципами створення, функціонування та можливостями ДІППК.
3. Використати можливості платформи для створення пакету документів, передбачених переддоговірними стосунками.

Теоретичний матеріал.

Переддоговірні стосунки передбачають попередні домовленості між сторонами перед укладенням основного договору.

Основними документами є:

- попередній договір,
- оферта
- акцепт.

Попередній договір має містити основні умови майбутньої угоди, терміни укладення основного договору, відповідальність за ухилення. Важливо чітко визначити предмет, ціну, умови виконання зобов'язань. Потрібно перевірити, чи відповідає він вимогам Цивільного кодексу України, зокрема статті 635.

Оферта — це пропозиція укласти угоду, яка має бути достатньо конкретною. Вона повинна включати всі істотні умови: предмет, ціну, строки.

Акцепт — це беззастережна згода на оферту. Треба вказати спосіб та термін акцепту, щоб уникнути суперечок.

ЗАВДАННЯ.

1) Виконати алгоритм організації переддоговірних стосунків.
2) Отримані документи зберегти у папці на власному гугл диску.
3) Для перевірки викладачеві створити єдиний документ з:

- нумерацією сторінок;
- колонтитулом (вказати дату створення та власне прізвище);
- закладками;
- гіперпосиланнями на пов’язану інформацію в документі;
- електронним змістом.

4) Документ підписати ЕЦП
5) Розмістити у класрумі під іменем ***Власне прізвище_4***

Організація переддоговірних стосунків: детальний алгоритм

1. Попередній договір (преконтракт)
2. Оферта (пропозиція укласти угоду)
3. Акцепт (прийняття пропозиції)
4. Протокол розбіжностей
5. Регламент переговорів
6. Додаткові механізми захисту
7. Зразок конфіденційної угоди

1. Умови для переговорів варто прописати окремо: конфіденційність, ексклюзивність переговорів, розподіл витрат. Це допоможе уникнути недопорозумінь. Також важливо на цьому етапі передбачити механізм вирішення спорів (переговори або медіація).

2. Звернути увагу на формальні вимоги: письмова форма попереднього договору, належне оформлення оферти та акцепту. Також варто передбачити санкції за порушення умов переддоговірних стосунків, наприклад, відшкодування збитків.

3. Додати зразки документів у вигляді артефактів, щоб користувач міг їх адаптувати. Важливо наголосити на необхідності юридичної експертизи перед підписанням, щоб уникнути правових ризиків.

4. Розглянути інші аспекти переддоговірних стосунків такі, як інформацію про електронні майданчики для переговорів, використання smart-контрактів, правові аспекти відповідно до чинного законодавства України, а також приклади додаткових документів, таких як лист-підтвердження намірів або угода про наміри.

5. Переконатися, що всі приклади документів відповідають українським юридичним нормам, вказати відповідні статті законів, якщо це можливо.

6. Вказати типові помилки під час укладення переддоговірних документів та запропонувати рекомендації щодо їх уникнення.

7. Передбачити використання системи електронного документообігу та використання ЕЦП.

Практична робота №5

Тема. Знайомство з основними функціями та можливостями пошуку та аналізу правової інформації у СІППС ActiveLex

Мета. Набути практичних компетенцій пошуку інформації в правовій аналітичній системі ActiveLex. Ознайомитися з основними розділами системи та опанувати послідовності виконання дій для роботи у кожному розділі.

1. База законодавства з актуальними змінами.
2. Судова практика — пошук рішень різних судів.
3. Шаблони документів (договори, заяви, накази).
4. Аналітичні матеріали та коментарі експертів.
5. Інструменти для моніторингу змін у законодавстві.

Підготувати презентацію з використанням екранних копій та коментарів для демонстрації послідовності роботи з кожним розділом системи.

Файл зберегти під іменем ***Власне прізвище_5*** та розмістити у Класрумі

ПРАКТИЧНА РОБОТА №6

Тема. Вирішення правових ситуацій засобами Інформаційно-пошукової спеціалізованої юридичної системи ЛІГА:360.

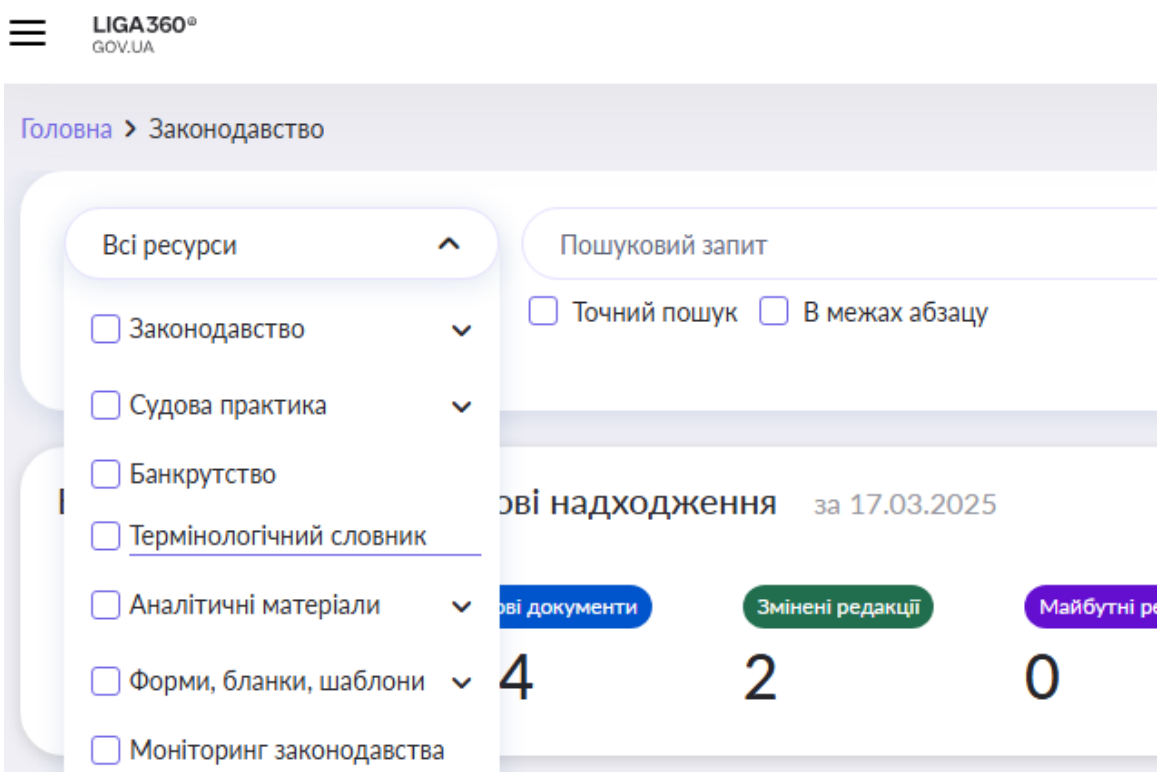
Мета. Ознайомитись з інтерфейсом ІПС Ліга:360, визначити перелік послуг за запропонованими вкладками.

Хід роботи.

ІПС Ліга:360 найповніше джерело систематизованої та достовірної правової інформації зі зручними інструментами для пошуку інформації. Дозволяють швидко знайти та проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію і прийняти правильне рішення.

Зайти на портал Ліга:36 https://zakon-pro.ligazakon.net/ за визначеним акаунтом.

Послідовно виконати дії для реєстрації. Відкриється вкладка Головна.



Завдання. Проаналізувати вміст запропонованих вкладок. Отримати конкретну інформацію за власним запитом. Результати відобразити в таблиці.

1. Закон України «Про авторське право і суміжні права.»
2. Проект закону України «Про внесення змін до деяких законодавчих актів щодо особливості регулювання земельних відносин для забезпечення швидкої реалізації інвестиційних проектів, спрямованих на відновлення економіки України під час дії воєнного стану та у відбудовний період.»
3. Постанова Верховної Ради України «Про структуру бюджетної класифікації України».
4. Наказ Міністерства охорони здоров'я України про «Єдиний перелік біологічних агентів, які становлять або можуть становити небезпеку для здоров'я людини».
5. Знайти за допомогою функціоналу відкритих даних «Законодавство України» 3 нормативно-правових акти, які належать до кримінально-виконавчого законодавства
6. Знайти за допомогою функціоналу відкритих даних «Законодавство України» угоди про співробітництво між Україною та іншими країнам в різних сферах (мінімум 3 приклади).
7. Навести з використанням інформаційно-пошукової бази даних «ЛІГА:360» 5 прикладів нормативно-правових актів, що втратили чинність у 2024 році.
8. Зробити з використанням інформаційно-пошукової бази даних «ЛІГА:360» добірку із 3 статей за певною сферою (напр. кримінальне право, кримінальний процес, адвокатура, нотаріат).

Результати пошуку занести у таблицю. В Стовпчику ПРИМІТКА описати особливості отриманого документа.

Практичні заняття 7-8

Тема 4. Організація та налаштування електронного документообігу

Практична робота 7-8

Тема. Створення електронного договору з використанням СІППС ЛІГА 360. Використання можливостей системи для розв'язання правових ситуацій.

Мета. Опанувати основні можливості ЛІГА:360: базу законодавства з актуальними змінами; судову практику – пошук рішень різних судів; шаблони документів (договори, заяви, накази); аналітичні матеріали та коментарі експертів; інструменти для моніторингу змін у законодавстві для вирішення практичних ситуацій. Створити електронний договір для подальшого використання в СЕД

Завдання 1. Підготувати договір поставки з урахуванням змін у ЦК України

1. Знайти шаблон договору поставки через фільтр «Договори».
2. Використати інструмент «Порівняння редакцій», щоб перевірити нові норми ст. 715 ЦК.
3. Вставити умови клієнта (оплата 50% авансу, штрафи за прострочення).
4. Перевірити документ на відповідність Закону «Про публічні закупівлі» через вбудований аналіз.

Варіанти додаткових умов:

Варіант 1. Замовник вимагає **100% передоплату** – ризик порушення ст. 715 ЦК України (максимальний аванс 50%).

Варіант 2.Постачальник пропонує **відстрочку платежу на 90 днів** –необхідно перевірити на відповідність Закону «Про дебіторську заборгованість».

Варіант 3.У договорі **відсутні санкції за прострочення** – автоматизувати розрахунок штрафу через шаблон ЛІГА 360.

Завдання 2. Підготувати захист клієнта у справі про стягнення заборгованості

1. Ввести у пошук судової практики ключові слова: *"стягнення заборгованості", "ФОП", "2024 рік", "Одеський апеляційний суд"*
2. Відфільтрувати рішення на користь позивача.
3. Скористатися аргументацією зі справи № 123/456 для підготовки позовної заяви.
4. Додати посилання на п. 45 Постанови Пленуму ВСУ № 8 у мотивувальній частині.

Варіанти додаткових умов:

Варіант 1.Позивач **не має письмового договору** – шукати в судовій практиці аналоги з п. 3 ст. 207 ЦК (усні домовленості).

Варіант 2.Відповідач **сплатив 70% суми** – використати фільтр рішень за ключовим словом «часткова компенсація».

Варіант 3.**Минув термін позовної давності** – перевірити можливість відновлення терміну через архів судових рішень.

Завдання 3. Підготувати консультування клієнта щодо змін у Податковому кодексі

1. У розділі «Зміни в законах» знайти останні поправки до ПКУ (грудень 2024).
2. Перевірити коментарі експертів до ст. 14.1.222 (пільги для ІТ-сектора).
3. Сформувати звіт для клієнта з використанням шаблону «Податкові зміни 2025».

Варіанти додаткових умов:

Варіант 1. Клієнт – **ІТ-компанія** – перевірити актуальні пільги за ст. 14.1.222 ПКУ (знижена ставка 9%).

Варіант 2. **Відшкодування ПДВ** – автоматизувати розрахунок через формулу в шаблоні ЛІГА 360.

Варіант 3. **Нова звітність для ФОП** – сформувати календар подачі документів з мобільним нагадуванням.

Завдання 4. Оскарження рішення податкової у господарському суді

1. Знайти у базі рішення ВСУ за запитом: *"оскарження податкового повідомлення", "неправомірне нарахування штрафу"*

2. Експортувати цитати з ухвал на користь платника податків у форматі Word.
3. Скористатися конструктором позовної заяви, підставивши дані клієнта.
4. Додати посилання на статтю 124 ПКУ через інтегрований підказник норм.

Варіанти додаткових умов:

Варіант 1. Податківець **не отримав повідомлення** – знайти прецеденти зі скасуванням штрафів через порушення п. 2 ст. 52 ПКУ.

Варіант 2. **Неправомірний штраф 500 000 грн** – використати калькулятор пені в ЛІГА 360 для перевірки розрахунків.

Варіант 3. **Порушення процедури перевірки** – знайти рішення ВСУ з анулюванням рішень через відсутність відеозапису.

Алгоритм роботи з умовами:

1. **Ідентифікація проблеми** → Пошук у базі ЛІГА 360 за ключовими словами.
2. **Аналіз прецедентів** → Фільтрація рішень на користь клієнта.
3. **Інтеграція рішення** → Використання шаблонів документів з автоматичним заповненням.

Практична робота № 9

Тема. Організація та налаштування електронного документообігу для юридичної фірми

Мета заняття: Навчити студентів основам роботи з системами електронного документообігу (ЕДО), від налаштування системи до управління документами та інтеграції з іншими бізнес-процесами юридичної фірми.

Обладнання та ресурси:

- Комп’ютери з доступом до інтернету.
- Встановлене програмне забезпечення для ЕДО (наприклад, M.E.Doc, Вчасно, Шрифт).
- Шаблони документів (контракти, заяви, звіти).
- Навчальні інструкції та відеоуроки.

Хід виконання практичної роботи

1. Пояснити, що таке електронний документообіг, його переваги та виклики.
2. Представити обрані програмні засоби для ЕДО (наприклад, їх функції, можливості та типові сценарії використання).
3. Ознайомити студентів із нормативно-правовими актами, які регулюють використання ЕДО в юридичній сфері.

Завдання

1. Зареєструватися у вибраній системі ЕДО.
2. Визначити ролі користувачів у системі (адміністратор, співробітник, клієнт).
3. Налаштувати базові параметри (мова, валюта, параметри безпеки).
4. Завантажити пакет документів (наприклад, переддоговірні документи, контракт).
5. Перевірити необхідні дані документа.
6. Розробити сценарій проходження документа в системі.
7. Визначити етапи проходження документа (від створення до затвердження).
8. Призначити відповідальних осіб і встановити терміни виконання.
9. Відслідковувати та аналізувати стан документа (затверджений, очікує підпису, відхилений).
10. Підписати документ електронним підписом.
11. Надіслати документ іншому користувачеві системи для затвердження.
1. Демонстрація можливостей інтеграції з CRM-системами або хмарними сховищами (наприклад, Google Drive, Dropbox).

2. Створення резервної копії документів у хмарному сховищі.
3. Розробка структури електронного архіву для юридичної фірми.

Очікувані результати. Після завершення роботи студенти повинні:

1. Розуміти, як налаштовувати систему електронного документообігу.
2. Вміти створювати, підписувати та обробляти електронні документи.
3. Знати, як інтегрувати ЕДО з іншими системами.
4. Оцінювати ефективність та безпеку використання ЕДО у юридичній практиці.

Послідовність виконання роботи відобразити в презентації. Файл зберегти під іменем ***Власне прізвище_8*** та розмістити у Класрумі

Тема 5. CRM-системи та їх роль у юридичному бізнесі

Практична робота № 10-11

Тема. Використання CRM систем у юридичній практиці

Мета. Ознайомитись з основами роботи CRM систем у юридичній сфері, набути компетенцій використання CRM для управління клієнтами, справами та автоматизації процесів в юридичній фірмі.

Необхідні ресурси:

- Комп'ютер або ноутбук з доступом до Інтернету
- Обліковий запис у безкоштовній CRM системі (наприклад, **KEY- срм**)
- Інтернет-браузер
- Мобільний телефон для можливого підтвердження акаунта (якщо потрібно)

Теоретична частина

1. Введення в CRM системи та їх застосування в юридичній практиці

Ознайомлення з CRM системами: customer relationship management (CRM), укр. сі-ар-ем) — поняття, що охоплює концепції, котрі використовуються компаніями для управління взаємовідносинами зі споживачами, включаючи збір, зберігання й аналіз інформації про споживачів, постачальників, партнерів та інформації про взаємовідносини з ними.

- що таке CRM система, її роль у бізнесі та юридичній діяльності.
- основні функцій CRM: управління клієнтами, автоматизація маркетингу, управління справами та документами, колаборація між співробітниками.
- переваги CRM для юридичних фірм: допомагає покращити взаємодію з клієнтами, підвищити ефективність і зменшити ризик помилок; дозволяє вести історію взаємодій із клієнтами, автоматизувати розподіл завдань та нагадування.

Вибір CRM системи:

- Обрати одну з безкоштовних CRM платформ для практичної роботи (наприклад, **KEY, СВОЯ**).
- Зареєструвати акаунт в CRM системі та ознайомитися з її основними функціями.

Заповнити форму реєстрації, вказати:

- ім'я та прізвище — ввести ім'я та прізвище тієї людини, яка буде головною в системі (зазвичай власник компанії, керівник). Саме їй будуть належати максимальні права доступу до CRM-системи.
- e-mail — на цю електронну пошту буде надіслано посилання для входу в акаунт та кабінет. А також логіни та паролі для доступу. Будь ласка, збережіть дані, щоб вони завжди були під рукою.
- номер телефону — на нього відправиться SMS із кодом підтвердження, який потрібно буде ввести на сторінці для підтвердження.

Вказати назву для CRM. Назва повинна складатися з латинських літер, вона відображатиметься в кабінеті системи, а також в URL посиланні (веб-адреса сторінки, до якої ви будете отримувати доступ).

Зверніть увагу! Наразі змінити назву неможливо. Тому, будь ласка, уважно заповнюйте це поле!

Вхід в акаунт та кабінет. Через кілька секунд після успішної реєстрації буде створено акаунт та кабінет, а всі дані для входу надіслано на вказаний e-mail.

Зверніть увагу! Якщо ви не знаходите листа у «Вхідних», будь ласка, перевірте розділ «Промоакції» та «Спам».

2. Налаштування CRM системи

Ознайомитись з Інтерфейсом CRM системи: основні елементи інтерфейсу обраної CRM системи: панель управління, списки контактів, робочі процеси, календар, звіти; Можливості роботи у різних розділах системи: «Клієнти», «Завдання», «Проекти», «Договори» тощо.

Створити облікові записи клієнтів (формування клієнтської бази):

- ввести у CRM систему кілька тестових облікових записів клієнтів (можна використовувати вигадані імена та дані).
- Для кожного клієнта створити записи: контактна інформація, тип справи, історія взаємодій, пріоритети та інші відомості.

Додавання та управління справами:

- додати кілька справ до CRM (наприклад, справи по юридичних консультаціях, угодах, судах).
- Розподілити справи між членами команди (групова робота).
- Визначити терміни виконання завдань, прикріпити документи.

Налаштування нагадувань та подій:

- налаштувати автоматичні нагадування про важливі події (наприклад, судові засідання, терміни подання документів).
- Визначити дедлайни для кожної справи та встановити відповідальних.

Послідовність виконання роботи відобразити в презентації. Файл зберегти під іменем ***Власне прізвище_10*** та розмістити у Класрумі

Тема 6. Кіберзлочинність та правове регулювання

Практична робота № 12

Тема. Розробка політики кібербезпеки для юридичної організації

Мета заняття: Ознайомлення з основами розробки політики кібербезпеки, специфічними вимогами для юридичних організацій та практичним застосуванням знань.

Завдання:

1. Розробити проект політики кібербезпеки для вигаданої юридичної організації, зосередившись на специфічних загрозах.
2. Визначити основні загрози.
3. Сформулювати цілі політики.
4. Написати короткий план реагування на інциденти.

Зразок проекту політики кібербезпеки для юридичної організації

Політика кібербезпеки

Юридична організація "Право та Безпека"

Дата набрання чинності: [Дата]
ЗАТВЕРДЖЕНО: [Ім'я керівника]
Дата: [Дата]

1. Вступ

Ця політика кібербезпеки визначає основні принципи, процедури та обов'язки для захисту інформаційних активів юридичної організації "Право та Безпека". Політика спрямована на забезпечення конфіденційності, цілісності та доступності даних.

2. Цілі політики

- Захист інформаційних активів організації від несанкціонованого доступу.
- Забезпечення відповідності законодавству та нормативним вимогам.
- Встановлення процедур реагування на інциденти.
- Підвищення обізнаності співробітників щодо кібербезпеки.

3. Оцінка ризиків

- Проведення регулярних оцінок ризиків для виявлення потенційних загроз.
- Оцінка впливу на бізнес у випадку порушення безпеки даних.
- Визначення заходів для зменшення ризиків.

4. Ролі та відповідальності

- **Керівництво:** Затвердження політики та виділення ресурсів для її реалізації.
- **Відповідальний за безпеку інформації:** Координація заходів з кібербезпеки та навчання співробітників.
- **Співробітники:** Дотримання політики та участь у навчаннях з кібербезпеки.

5. Процедури реагування на інциденти

- Визначення категорій інцидентів (незаконний доступ, втрати даних тощо).
- Створення команди реагування на інциденти.
- Процедури повідомлення про інциденти та їх розслідування.

6. Моніторинг і оновлення політики

- Регулярний моніторинг виконання політики.
- Оновлення політики відповідно до змін у законодавстві та технологіях.
- Проведення щорічних переглядів політики.

7. Підвищення обізнаності

- Проведення регулярних тренінгів для співробітників.
- Розробка інформаційних матеріалів з кібербезпеки.
- Створення каналу для зворотного зв'язку та запитань щодо кібербезпеки.

8. Висновок

Ця політика кібербезпеки є важливим документом для забезпечення безпеки інформаційних активів юридичної організації "Право та Безпека". Дотримання цієї політики є обов'язковим для всіх співробітників.

Зразок проекту політики кібербезпеки можна адаптувати відповідно до специфіки організації та її потреб.

Файл підписати ЕЦП, зберегти під іменем ***Власне прізаище_11*** та розмістити для перевірки у Класрумі

Практичні заняття 13-15

Тема 7. Електронне судочинство

1. Єдина судова інформаційно-телекомунікаційна система (ЄСІТС).
2. Модулі ЄСІТС. Офіційний веб-портал «Судова влада України».
3. Єдиний державний реєстр судових рішень.

4. Єдина підсистема управління фінансово-господарськими процесами. Єдиний контакт-центр судової влади України. Модуль «Автоматизований розподіл». Модуль «Судова статистика». Підсистема відеоконференцзв'язку.

5. Підсистема «Електронний суд».

6. Підсистема «Електронний кабінет».

7. Практичні аспекти подання процесуальних документів в електронній формі, включаючи реєстрацію в системі, створення, підписання та відправлення документів.

8. Оцінка переваг електронного судочинства, таких як оперативність, доступність та зручність роботи. Розгляд викликів і обмежень, пов'язаних із впровадженням електронного судочинства, зокрема технічних, організаційних та правових аспектів. Практичні завдання з моделювання подачі документів через систему «Електронний суд» та роботи з електронними доказами.

9. Практика підготовки та подання заяв до ЄСПЛ: основні вимоги, формати документів, електронна комунікація із секретаріатом.

10. Практичні аспекти моделювання подачі документів через систему «Електронний суд», підготовка заяви до ЄСПЛ та ознайомлення з ключовими інструментами міжнародних платформ для юристів.

Практичні заняття 16-17

Тема 8. Цифрові інструменти в юридичній практиці

1. Використання Legal Tech для автоматизації рутинних процесів.
2. Огляд популярних цифрових платформ для юристів (Luminance, Clio).
3. Інтеграція штучного інтелекту у юридичну діяльність.
4. Використання юридичних баз даних для пошуку нормативно-правових актів та судових рішень.
5. Практичні аспекти роботи з Єдиним державним реєстром судових рішень, базою національного законодавства, актів європейського та міжнародного права.
6. Комерційні продукти обробки законодавства та судової практики.
7. Оцінка релевантності та достовірності отриманої інформації.
8. Використання сучасних онлайн-платформ для автоматизації рутинних юридичних завдань.
9. Навчання основним прийомам роботи з цифровими інструментами, включаючи пошук, фільтрацію та аналіз інформації.
10. Практичні аспекти побудови ефективного алгоритму пошуку нормативних документів та судових рішень, використання цифрових інструментів для їх систематизації.

Тема 9. Мультимедійна підтримка юридичної діяльності

Практична робота №18

Тема. Створення ментальної карти в сервісі Coggle

Мета. Навчитися створювати структури подій, ситуацій та проектів та зображати їх у вигляді ментальної карти.

1. Відкрийте сторінку сервісу Coggle за посиланням https://coggle.it/, ознайомтеся з відомостями про сервіс на головній сторінці.

2. Натиснувши кнопку Sign Up Now або Log in (див. рис. 1), зареєструйтеся за допомогою вашого, облікового запису Google (див. рис. 2). Ознайомтеся з можливими тарифними планами та їх умовами.

Рисунок 1 - Реєстрація в сервісі Coggle

3. Після вибору тарифного плану відкривається персональна сторінка сервісу (див. рис. 3). В лівій частині вікна знаходяться основні три директорії, в яких зберігаються: 1) ментальні карти, створені вами; 2) ментальні карти, до яких вам відкрили доступ інші користувачі; 3) загальна галерея ментальних карт користувачів сервісу у відкритому доступі. Ознайомтеся з прикладами створення інтелект-карт в галереї.

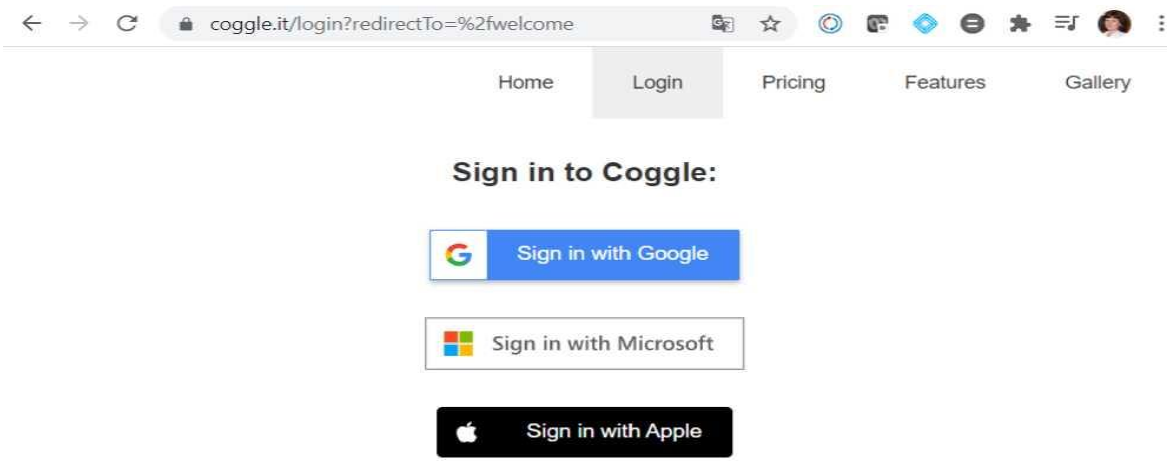


Рисунок 2 - Реєстрація за допомогою облікового запису Google

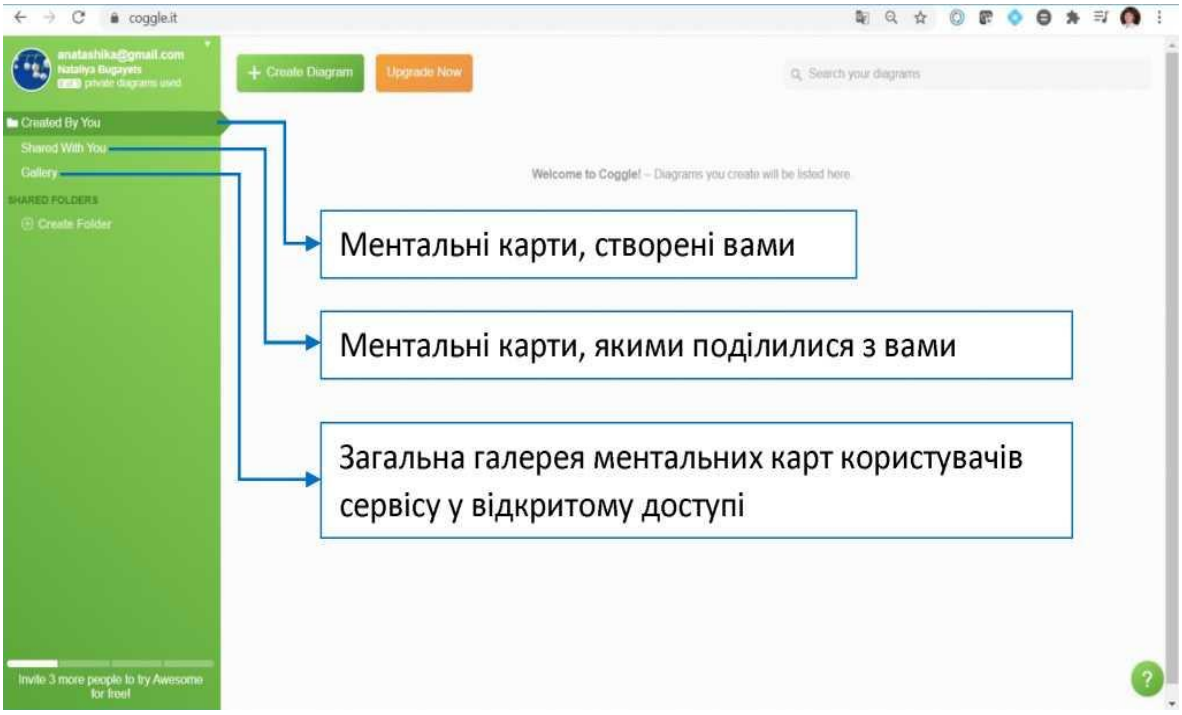


Рисунок 3 - Персональна сторінка сервісу Coggle

4. Для створення власної ментальної карти в директорії Created By You натисніть кнопку Create Diagram (див. рис. 3). З'явиться робоча область з центральним елементом ментальної карти. Для прикладу створимо карту знань про різні засоби хмарних сервісів у роботі вчителя. Вводимо центральний елемент - «Хмарні сервіси» (див. рис. 4).

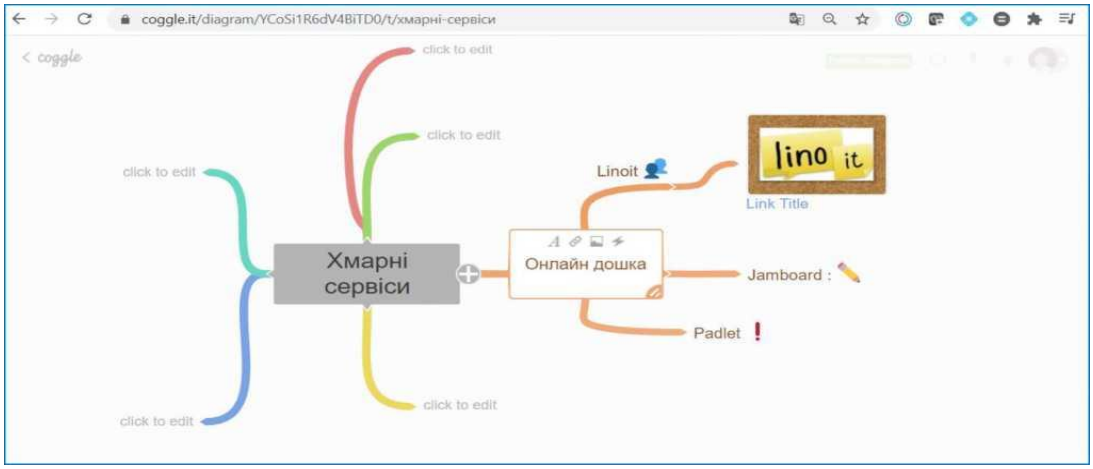


Рисунок 4 - Створення ментальної карти «Хмарні сервіси»

5. Натискаємо плюс, щоб створити відгалуження від центрального елементу. Пишемо назви категорії онлайн сервісів. Невдало виконану дію відміняють комбінацією клавіш Ctrl+Z.

6. Кожен ключовий елемент має набір послуг для форматування накреслення тексту, додавання посилань, зображень та піктограм (див. рис. 5).

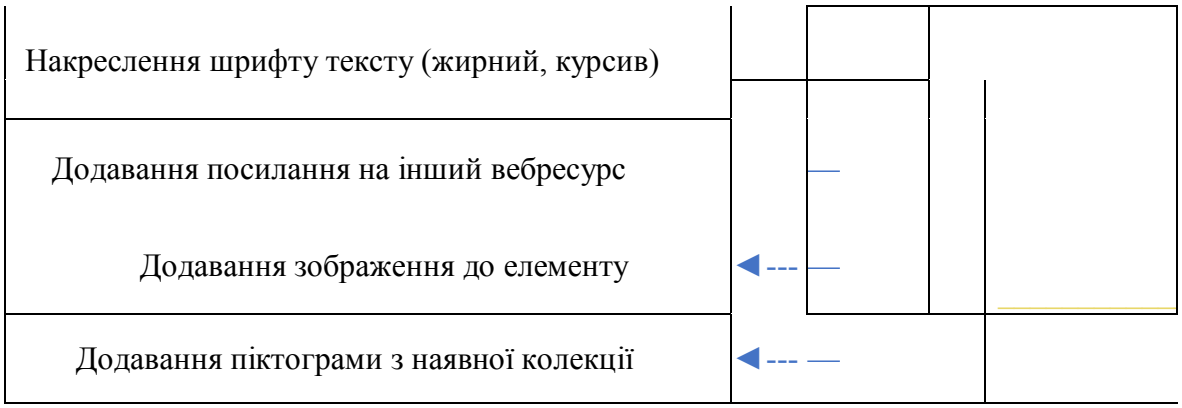


Рисунок 5 - Можливості при роботі з окремими елементами

7. В процесі додавання посилань чи зображень з'являється спеціальний текст розмітки, який зникає, якщо клацнути мишею за межами елементу (див. рис. 6).

8. Натискаючи і утримуючи ліву кнопку миші на вільному місці ментальної карти, її

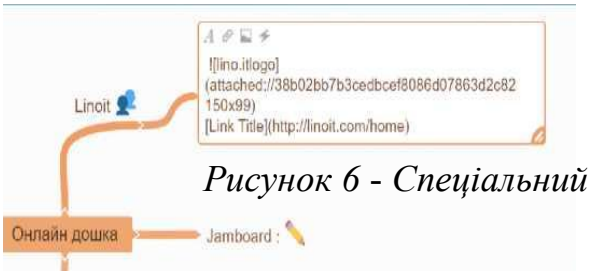
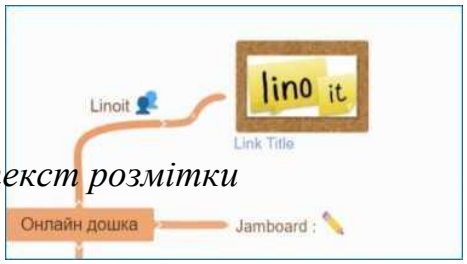


Рисунок 6 - Спеціальний текст розмітки



можна переміщувати.

9. Якщо навести вказівник миші на плюс, натиснути ліву кнопку і не відпускаючи її протягнути, то відгалуження розтягуються. Білі кружечки на гілках - це ключові вузли, за допомогою переміщення яких змінюють форму гілки.

10. Щоб видалити створений елемент гілки, наводять вказівник миші на плюс і утримуючи клавішу Alt, натискають хрестик, що з'являється замість плюса. Повний перелік можливих дій за допомогою комбінацій клавіш знаходиться на додатковій панелі, яка відкривається після натискання знаку питання в правому нижньому кутку екрану (див. *Повний перелік можливих дій за допомогою комбінацій клавіш)*

11. Щоб додати ключовий елемент ментальної карти між двома вже створеними елементами, потрібно навести вказівник миші на плюс перед елементом і натиснути клавішу Shift. Тоді плюс змінюється на стрілку, натиснувши яку лівою кнопкою миші створюємо новий елемент (див. рис. 8).

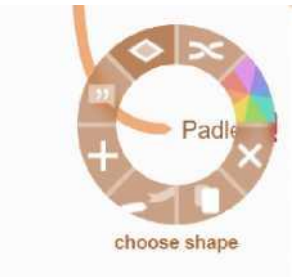
Онлайн дошка

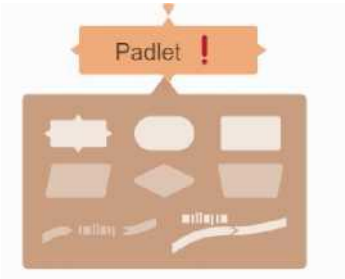
Padlet

клавіша Shift і ліва кнопка миші

Рисунок 8 - Додавання ключового елемента ментальної карти між двома вже створеними елементами

12. Якщо плюс натиснути правою кнопкою миші, то з'являється кругове меню. За допомогою choose shape ключовий елемент можна виділити у формі прямокутників (див. рис. 9). Деякі послуги цього меню недоступні в безкоштовній версії, зокрема налаштування кольору гілки.





13. Розгляньте послуги меню, що знаходиться справа вгорі вікна програми. Перша кнопка у вигляді екрану призначена для демонстрації створеної карти на весь екран.

Завдання до практичної роботи

1. Створіть слайд-візитівку в спільній Google-презентації. Посилання на презентацію знаходиться на сторінці електронного курсу або запитайте викладача. На слайді запишіть ваше прізвище, ім'я, по-батькові, шифр групи, додайте ваше фото, виконайте оформлення слайду згідно вимог до презентацій. Не змінюйте загальних налаштувань презентації, зокрема тему оформлення. Надалі цей слайд буде використовуватися для публікації посилань (див. рис. 11) на ваші виконані роботи.

2. Створіть ментальну карту (карту знань) за допомого сервісу Coggle на довільну тему за вашою спеціальністю. Карта повинна мати не менше трьох рівнів розгалужень, зображення, посилання та інші елементи оформлення. Згенеруйте посилання на цю карту та опублікуйте його на вашому слайді- візитівці спільної презентації.

ПРАКТИЧНА РОБОТА №19

Тема. Узагальнення систематизація та публікація матеріалів через сайт в он-лайн просторі.

Мета. Створити сайт через додаток Google.

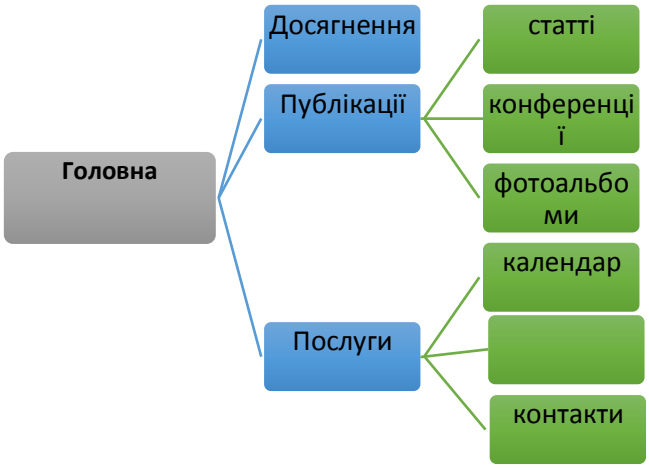
Хід виконання роботи

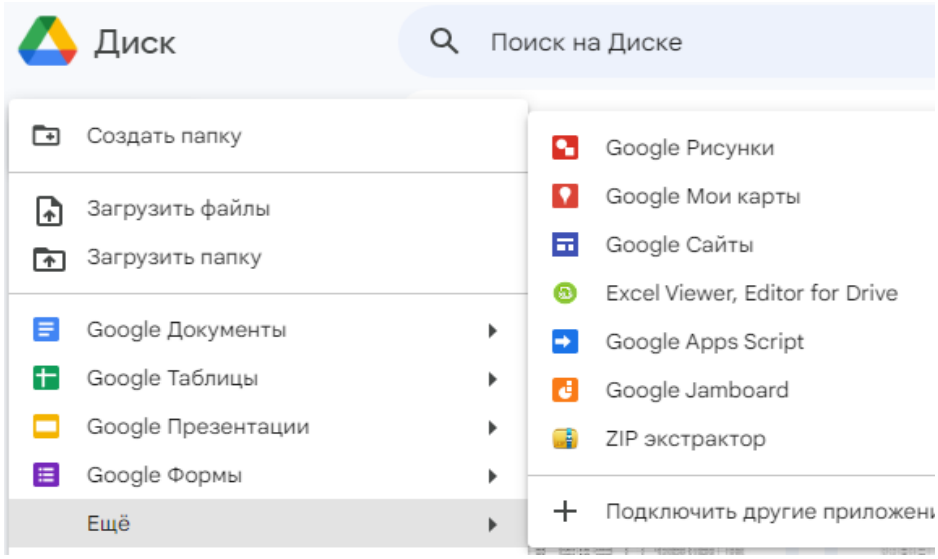
Додаток Google Сайт використовують для створення: персонального сайту (порт-фоліо), блогу; сайту установи чи організації; узагальнення матеріалів за проектом чи напрямком діяльності.

Щоб створити безкоштовний сайт Google, потрібно:

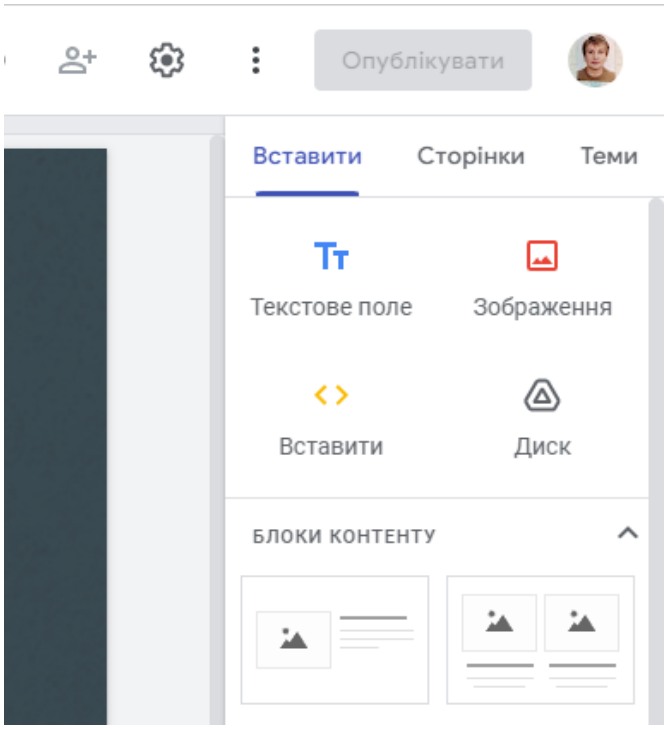
1. Підготувати макет майбутнього сайту.
2. Створити або зайти у свій акаунт Google.

3. В пошуковій стрічці набрати - Google Sites.
4. Натиснути на кнопку "Створити новий сайт".
5. Налаштувати оформлення - обрати шаблон та тему.
6. Заповнити назву сайту.
7. Додати контент.
8. Опублікувати.





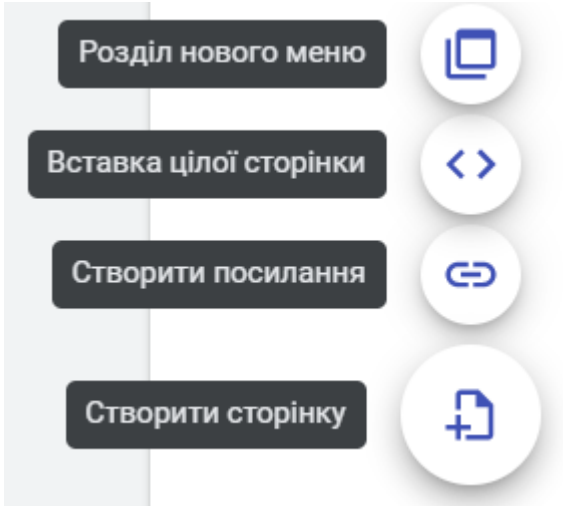
Навігація



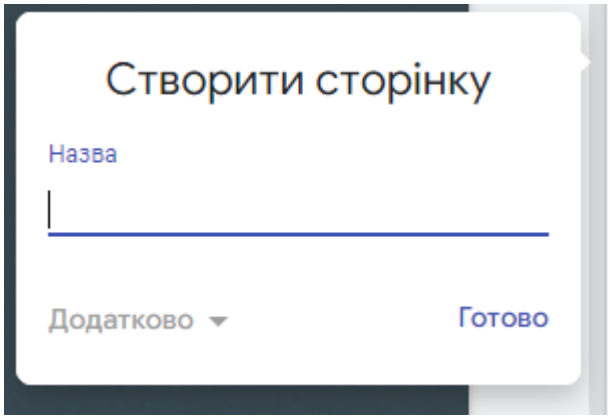
Для створення нової сторінки на сайті слід:

1). Вибрати заголовок вкладки Сторінки на бічній панелі в правій частині вікна.

2). Навести вказівник на кнопку  і вибрати кнопку Створити сторінку .



3). Увести назву сторінки в поле **Ім'я** у вікні Нова сторінка.

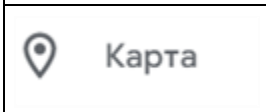


4). Клікнути посилання Готово.

Під час створення нових сторінок автоматично формується панель навігації
Порядок сторінок можна змінити, перетягнувши на вкладці Сторінки бічної панелі блок з назвою сторінки в потрібне місце.
Для створення головної сторінки тематичного розділу потрібно перетягнути блоки з назвами інших сторінок цього розділу на назву головної сторінки розділу.
Таким чином розробником сайту формуються структура сайту та панель навігації.
Вставлення об'єктів на вебсторінку
На вебсторінку можна вставити різні об'єкти: текстові поля, зображення, гіперпосилання, документи, які розміщено на Google Диску, та ін. Для цього призначено вкладку Вставити на бічній панелі. Усі об'єкти, які додаються на вебсторінку, розміщуються в окремих блоках. Кожен блок можна перемістити, змінити його розміри, використовучи маркери на межах, або видалити. Для кожного блока, якщо його вибрати, відкривається окрема панель налаштувань.

Призначення елементів керування вкладки Вставити

Елемент керування	Призначення
	Створення блока введення тексту. Текст може бути оформлений як Назва, Заголовок, Підзаголовок, Звичайний текст і Малий
	Уставлення зображення з Google Диска, за URL-адресою з Інтернету, з носіїв даних комп'ютера тощо
	Уставлення об'єктів різних типів з Інтернету за їх URL-адресою або вставлення фраг ментів HTML-коду
	Уставлення документів різних типів з Google Диска

	Вибір макета розміщення об’єктів на сторінці
	Створення змісту сторінки. Зміст формується автоматично із заголовків, розміщених у текстових полях на сторінці, та призначений для швидкого переходу до вибраного заголовка на поточній сторінці
	Створення слайд-шоу з вибраних зображень
	Уставлення кнопки
	Уставлення відео із сервісу YouTube
	Уставлення календаря, створеного в сервісі Google Календар
	Уставлення карти, створеної у сервісі Google Карти

Для видалення вставленого об’єкта потрібно вибрати кнопку Видалити в панелі налаштувань блока цього об’єкта.

Публікація сайту

Створений вами сайт буде залишатися недоступним для користувачів Інтернету, поки ви його не опублікуєте.

Для публікації слід:

- Вибрати кнопку Опублікувати у верхній частині вікна браузера.
- Увести, використовуючи малі літери латиниці, цифри та тире, останню частину URL-адреси сайту. Перша частина адреси (доменне ім’я сервера та шлях до файлу) для всіх сайтів буде однаковою: sites.google.com/view/FEDORCHUK. Остання частина повинна бути унікальною для кожного сайту.
- Вибрати кнопку Опублікувати.

Опублікований сайт можна переглянути, вибравши команду Переглянути опублікований сайт у списку кнопки Опублікувати. Адреса, яку потрібно повідомити користувачам Інтернету для перегляду вашого сайту, буде міститися в рядку адреси у вікні перегляду опублікованого сайту.

Після внесення будь-яких змін до вашого сайту його потрібно повторно опублікувати. Уведення URL-адреси сайту буде вимагатися лише під час першої публікації сайту.

За потреби можна скасувати публікацію, вибравши в списку
кнопки Опублікувати команду Скасувати публікацію. Сайт буде залишатися недоступним користувачам Інтернету до повторної його публікації.

1.3. Самостійна робота студентів

Самостійна робота студентів є важливою складовою частиною навчального процесу та має на меті закріплення та поглиблення знань і навичок, одержаних на усіх видах навчальних занять; підготовку до наступних занять, іспиту, формування культури розумової праці з чинними правовими нормами, законодавством та практикою його застування. Під час самостійної роботи уточнюється коло питань, що підлягають вивченню по темі, аналізується та вивчається нормативний матеріал, наукові джерела, виконуються завдання.

Самостійна робота студента виконується в позааудиторний час, передбачений тематичним планом навчальної дисципліни.

Під час вивчення навчальної дисципліни студенти повинні навчитися самостійно мислити, поглиблювати засвоєні теоретичні знання, опановувати практичні навики з організації праці менеджера. Відповіді на питання повинні бути стисло законспектовані з обов'язковими посилання на використані джерела.

Самостійна робота студентів має бути логічно пов'язана з іншими видами навчальних занять. Однак вивчення навчальної дисципліни чи окремої теми не бажано починати з самостійної роботи студентів.

Від якості самостійної підготовки студентів залежить якість семінарських занять, глибина їх теоретичного змісту й активність студентів.

Самостійна робота є методом глибокого вивчення і творчого засвоєння студентами навчальної програми.

Перевірка самостійної роботи студентів здійснюється викладачами, які проводять семінарські заняття з навчальної дисципліни.

Викладач може обрати один з наступних способів перевірки самостійної роботи:

- проведення перевірки конспектів опрацьованої літератури, яка рекомендується для вивчення теми навчальної дисципліни;
- фронтального усного опитування;
- письмового опитування;
- проведення тестування з вивчених тем;
- виконання практичних завдань до кожної теми навчальної дисципліни.

З метою самостійного визначення рівня засвоєння теоретичного матеріалу студентам пропонуються питання для самоконтролю набутих знань.

Питання самостійної роботи виносяться на поточний і підсумковий семестровий контроль. Для самостійної роботи студентів з кожної теми надається рекомендована література з якою студенти повинні ознайомитися для якісного виконання завдань на самостійну підготовку.

Загальні методичні рекомендації щодо самостійної роботи студентів:

1. Ознайомитися із питаннями, що виносяться на самостійне вивчення студентами.
2. Ознайомитися із рекомендованими джерелами до відповідної теми.
3. За бажанням студент може підготувати коротке повідомлення (до десяти хвилин) з найбільш складного і цікавого питання.
4. У випадку необхідності студент може скористатися індивідуальними консультаціями викладача, який читає лекції, а також викладача, який проводить семінарські заняття у навчальній групі.

Тема 1. Вступ до інформаційно-комунікаційних технологій у праві

Ознайомлення з основами цифровізації у правничій діяльності. Значення впровадження інформаційно-комунікаційних технологій для підвищення ефективності роботи юристів. Практичний аналіз переваг цифрових рішень, таких як автоматизація процесів, покращення комунікації та доступ до інформації. Розгляд викликів, зокрема ризиків кібербезпеки та проблем адаптації нових технологій. Законодавче регулювання використання ІКТ у правничій сфері в Україні. Практичні завдання включають аналіз кейсів із впровадження ІКТ у юридичній діяльності та створення індивідуального плану цифровізації для юридичної фірми чи проєкту.

Тема 2. Робота з даними у юридичній практиці

1. Оцінити політику конфіденційності сайтів та реєстрів. Визначити основні критерії конфіденційності. Опрацювати по три сайти і три реєстри. Дані занести в таблицю.
2. Створити перелік основних реєстрів та цифрових додатків для роботи ФОП різних груп
3. Створити перелік основних реєстрів та цифрових додатків для роботи юридичних осіб.
4. Отримати сертифікат про проходження курсу (на вибір):
   - «Медіаграмотність для громадян» за посиланням https://irex.mocotms.com/
   - «Very Verified: онлайн-курс з медіаграмотності» за посиланням: https: //verified.ed-era.com/ua

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: бази даних, відкриті дані та юридичні дослідження (due diligence), Портал відкритих даних, персональні дані, політика конфіденційності, безпека персональних даних.

***З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах*:**

1. Основні поняття та законодавчі основи

Персональні дані – це інформація, яка стосується конкретної особи, яку можна ідентифікувати прямо або непрямо. Це може включати ім'я, прізвище, адресу, номер телефону, електронну пошту, дані про освіту, зайнятість тощо. Персональні дані можуть бути простими, наприклад, ім'я та прізвище, або складними, наприклад, біометричні дані або інформація про здоров'я.

Персональні дані можна розділити на декілька категорій, залежно від їхньої чутливості та потенційного впливу на особу. До цих категорій належать: загальні персональні дані (ім'я, адреса тощо), спеціальні категорії персональних даних (інформація про расу, релігію, здоров'я тощо), та біометричні дані (відбитки пальців, обличчя тощо).

Захист персональних даних є критично важливим для підтримки довіри між особами та організаціями, які обробляють ці дані. Несанкціонований доступ, зміна або знищення персональних даних може привести до серйозних наслідків, включаючи фінансові збитки, пошкодження репутації та психологічний дискомфорт для осіб, яких це стосується.

Безпека персональних даних

Безпека персональних даних відноситься до комплексу заходів, спрямованих на захист персональних даних від несанкціонованого доступу, зміни, знищення або іншого неправомірного використання. Це включає використання технічних, організаційних та правових заходів для забезпечення конфіденційності, цілісності та доступності персональних даних.

Ефективна безпека персональних даних складається з трьох основних компонентів: конфіденційності (забезпечення, що дані не будуть доступні неповноваженим особам), цілісності (забезпечення точності та повноти даних) та доступності (забезпечення, що дані будуть доступні авторизованим особам, коли це необхідно).

У сучасному цифровому середовищі, безпека персональних даних стикається з численними викликами, включаючи зростаючу кількість кібератак, розвиток нових технологій (наприклад, IoT, штучний інтелект) та підвищені вимоги до захисту даних з боку законодавства та регуляторів.

Законодавчі основи в Україні

Закон України "Про захист персональних даних" (2010): Це основний законодавчий акт, який регулює обробку персональних даних в Україні. Закон встановлює вимоги до обробки персональних даних, права осіб, яких ці дані стосуються, та відповідальність за порушення законодавства.

Генеральний регламент про захист даних (GDPR): Хоча GDPR є законодавчим актом Європейського Союзу, він також застосовується до українських компаній, які обробляють персональні дані громадян ЄС. Це означає, що українські організації, які працюють з клієнтами з ЄС, повинні відповідати вимогам GDPR щодо захисту персональних даних.

Інші релевантні закони та норми: Крім Закону про захист персональних даних, інші українські законодавчі акти та міжнародні стандарти (наприклад, закон про захист інформації в інформаційно-телекомунікаційних системах) також можуть застосовуватися до захисту персональних даних в залежності від конкретного контексту обробки даних.

2. Принципи обробки персональних даних у юридичній діяльності

Принцип Законності. Обробка персональних даних повинна здійснюватися на законних підставах, тобто відповідно до законодавства України та міжнародних зобов'язань. Це означає, що організація повинна мати причину для обробки даних, яка відповідає встановленим законодавчим вимогам.

Законні підстави для обробки персональних даних можуть включати згоду особи, виконання договору, виконання законодавчих обов'язків, захист життєво важливих інтересів особи чи інших осіб, а також виконання завдань, що здійснюються в публічних інтересах або під час здійснення офіційних повноважень.

Організації несуть відповідальність за забезпечення законності обробки персональних даних. Це включає проведення оцінки впливу на захист даних (DPIA) для нових процесів обробки даних, які можуть становити високий ризик для осіб, яких ці дані стосуються.

Принцип відповідності. Метою обробки персональних даних повинна бути досягнення конкретної, rõчно визначеної мети. Це означає, що організація повинна чітко визначити, навіщо їй потрібні дані, і гарантувати, що дані обробляються лише для цієї мети.

Метою обробки може бути виконання договору, надання послуг, маркетингова діяльність тощо. Організації повинні документувати мету обробки даних і забезпечити, щоб усі співробітники, хто обробляє дані, розуміли цю мету.

Принцип відповідності тісно пов'язаний з принципом мінімалізації. Якщо дані не потрібні для досягнення мети, їх не слід обробляти. Це допомагає зменшити ризики для осіб, яких дані стосуються, та підвищити загальний рівень захисту даних.

Принцип мінімалізаці. Обсяг оброблюваних персональних даних повинен бути мінімальним, необхідним для досягнення мети обробки. Це означає, що організація повинна обробляти лише ті дані, які абсолютно необхідні для виконання своєї задачі.

Організації повинні регулярно проводити оцінку необхідності обробки персональних даних. Якщо дані більше не потрібні для досягнення мети, їх слід видалити або анонімізувати, щоб уникнути подальшої обробки.

Мінімалізація даних може включати збір тільки необхідної інформації під час реєстрації клієнтів, обмеження доступу до даних лише для тих співробітників, яким це необхідно, та використання псевдонімів або анонімізації даних, коли це можливо.

Принцип точності та достовірності. Персональні дані повинні бути точними та актуальними. Це означає, що організація повинна гарантувати, що дані, які вона обробляє, правильні та оновлені, щоб уникнути помилок або неправдивої інформації.

Організації повинні встановити механізми для підтримки точності даних, включаючи регулярні перевірки даних, надання можливості особам оновлювати свої дані та виправляти помилки, якщо вони виявлені.

Організації несуть відповідальність за точність даних, які вони обробляють. Якщо виявлені помилки, організації повинні негайно виправити їх, щоб уникнути потенційних наслідків для осіб, яких дані стосуються.

Принцип обмеження терміну зберігання. Персональні дані повинні зберігатися не довше, ніж це необхідно для досягнення мети обробки. Це означає, що організація повинна встановити чіткі терміни зберігання даних та дотримуватися їх, щоб уникнути необґрунтованого тривалого зберігання даних.

Організації повинні чітко визначити терміни зберігання даних для різних категорій даних, залежно від їхньої мети обробки. Ці терміни повинні бути документовані та доступні для всіх співробітників, хто обробляє дані.

Після закінчення терміну зберігання даних організації повинні мати встановлені процедури для безпечного видалення даних, щоб уникнути потенційних ризиків для осіб, яких дані стосуються.

Принцип інтеграції захисту. Захист персональних даних повинен бути інтегрований у процес обробки даних від початку до кінця. Це означає, що організація повинна враховувати вимоги захисту даних на всіх етапах обробки даних, від збір даних до їх видалення.

Інтеграція захисту може включати проведення оцінки впливу на захист даних (DPIA) для нових процесів обробки даних, розробку безпеки за замовчуванням та за замовчуванням, забезпечення прозорості обробки даних для осіб, яких дані стосуються.

Організації повинні сприяти культурі захисту даних серед своїх співробітників, забезпечуючи належну освіту та тренування щодо вимог захисту даних та найкращих практик обробки персональних даних.

Принцип трансперантності. Організації повинні забезпечити прозорість обробки персональних даних, надавши особам, яких дані стосуються, ясну та доступну інформацію про обробку їхніх даних.

Організації повинні надавати інформацію про обробку даних, включаючи:

Мету обробки. Види оброблюваних даних. Термін зберігання даних. Права осіб, яких дані стосуються. Контактну інформацію відповідальної особи.

Організації можуть підвищити прозорість обробки даних шляхом: Публікації політики обробки даних на сайті. Надання інформованих згод на обробку даних. Створення спеціальної сторінки з інформацією про обробку даних

Принцип відповідальності. Організації несуть відповідальність за дотримання принципів обробки персональних даних та забезпечення захисту даних.

Організації повинні встановити механізми для забезпечення відповідальності, включаючи: Призначення відповідальної особи з захисту даних. Створення політики обробки даних. Регулярний аудит та оцінка системи обробки даних. Надання звітів про інциденти з обробкою даних. Організації несуть відповідальність за несанкціонований доступ до персональних даних та зобов'язані повідомити особи, яких дані стосуються, у разі інциденту.

Принцип співпраці. Організації повинні співпрацювати з іншими організаціями, регуляторними органами та особами, яких дані стосуються, для забезпечення захисту персональних даних.

Організації можуть співпрацювати шляхом:

Обміну інформацією про кращі практики захисту даних

Участі в спільних проєктах з підвищення безпеки даних

Надання допомоги у разі інцидентів з обробкою даних

Співробітництва з регуляторними органами для забезпечення дотримання законодавства

Співпраця може принести такі бенефіти, як підвищення рівня захисту даних, зменшення ризиків та покращення репутації організації.

3. Права осіб, яких стосуються дані

Право на інформування. Особи, яких дані стосуються, мають право на отримання ясної та доступної інформації про обробку їхніх даних.

Організації повинні надавати інформацію про: Мету обробки. Види оброблюваних даних. Термін зберігання даних. Права осіб, яких дані стосуються.

Організації можуть інформувати особи шляхом: Публікації політики обробки даних на сайті. Надання інформованих згод на обробку даних Відправки повідомлень електронною поштою або поштою.

Право на доступ до даних. Особи, яких дані стосуються, мають право на доступ до своїх персональних даних, оброблюваних організацією.

Організації повинні надавати інформацію про: Види оброблюваних даних. Мету обробки. Термін зберігання даних. Права осіб, яких дані стосуються.

Організації повинні встановити процедуру доступу до даних, яка буде ясною та доступною для осіб, яких дані стосуються.

Право на виправлення даних. Особи, яких дані стосуються, мають право на виправлення своїх персональних даних, якщо вони є невірними або неповними.

Організації повинні встановити процедуру виправлення даних, яка буде ясною та доступною для осіб, яких дані стосуються.

Організації повинні виправити дані у розумний термін після отримання запитів від осіб, яких дані стосуються.

Право на видалення даних. Особи, яких дані стосуються, мають право на видалення своїх персональних даних, якщо вони більше не потрібні для мети обробки.

Організації повинні видалити дані в таких випадках: Дані більше не потрібні для мети обробки. Особа, яку дані стосуються, відкликала свою згоду. Обробка даних є незаконною. Видалення даних є обов'язковим відповідно до законодавства. Організації повинні встановити процедуру видалення даних, яка буде ясною та доступною для осіб, яких дані стосуються.

Право на обмеження обробки. Особи, яких дані стосуються, мають право на обмеження обробки своїх персональних даних в певних випадках.

Організації повинні обмежити обробку даних в таких випадках: Особа, яку дані стосуються, оскаржує точність даних. Обробка даних є незаконною, але особа, яку дані стосуються, не хоче видалити дані. Організації більше не потрібні дані для мети обробки, але особа, яку дані стосуються, потребує їх для захисту своїх інтересів. Організації повинні встановити процедуру обмеження обробки даних, яка буде ясною та доступною для осіб, яких дані стосуються.

Право на перенесення даних. Особи, яких дані стосуються, мають право на перенесення своїх персональних даних до іншої організації.

Організації повинні дозволити перенесення даних в таких випадках: Обробка даних здійснюється на підставі згоди особи або виконання договору. Обробка даних здійснюється автоматизованими засобами.

Організації повинні надати дані в структурованому, широко використовуваному та машинному форматі.

Право на відмову від автоматизованого рішення. Особи, яких дані стосуються, мають право на відмову від участі в автоматизованому процесі прийняття рішень, яке має юридичні наслідки або суттєвий вплив на особу.

Організації повинні дозволити відмову від автоматизованого рішення в таких випадках: Рішення має юридичні наслідки. Рішення має суттєвий вплив на особу. Рішення не ґрунтується на згоді особи або виконання договору. Організації повинні встановити процедуру відмови від автоматизованого рішення, яка буде ясною та доступною для осіб, яких дані стосуються.

4. Захист Персональних даних у юридичній діяльності

Технічні та організаційні міри захисту. Організації повинні імплементувати технічні та організаційні міри для захисту персональних даних.

Приклади міри захисту:

- Шифрування даних
- Контроль доступу
- Резервне копіювання даних
- Охорона мережі та систем

Оцінка ефективності міри захисту: Організації повинні регулярно оцінювати ефективність імплементованих міри захисту та вносити необхідні корективи.

Інциденти з обробкою даних

Інцидент з обробкою даних - це подія, яка призвела до порушення безпеки персональних даних.

Процедура реагування на інциденти:

- Виявлення інциденту
- Оцінка впливу інциденту
- Виправлення інциденту
- Інформування осіб, яких дані стосуються, та регуляторних органів

Документування інцидентів: Організації повинні документувати інциденти з обробкою даних та зберігати записи про інциденти протягом встановленого терміну.

Повідомлення про інциденти з обробкою даних. Організації повинні повідомити регуляторні органи про інциденти з обробкою даних у термін не пізніше 72 годин після виявлення інциденту.

Організації повинні надати регуляторним органам інформацію про: Характер інциденту. Кількість та категорію осіб, яких дані стосуються. Кількість та види персональних даних, які були порушені. Міри, які були вжиті для виправлення інциденту. Організації повинні повідомити осіб, яких дані стосуються, про інциденти з обробкою даних, якщо інцидент може призвести до високого ризику для їхніх прав і свобод.

Аудит та оцінка безпеки даних. Організації повинні проводити регулярний аудит своєї системи обробки даних для забезпечення дотримання законодавства та стандартів безпеки.

Організації повинні оцінювати ефективність своїх заходів безпеки та вносити необхідні корективи для забезпечення захисту персональних даних.

Організації повинні складати звіт про аудит та оцінку безпеки даних та зберігати його протягом встановленого терміну.

Підготовка до реагування на інциденти. Організації повинні розробити план реагування на інциденти з обробкою даних, який буде передбачати процедури для виправлення інциденту та мінімізації його впливу.

Організації повинні забезпечити навчання свого персоналу щодо процедур реагування на інциденти з обробкою даних.

Організації повинні періодично перевіряти свій план реагування на інциденти з обробкою даних та оновлювати його відповідно до потреб.

5. Міжнародний трансфер персональних даних

Загальні принципи міжнародного трансферу. Міжнародний трансфер персональних даних - це передача даних між організаціями, розташованими в різних країнах.

Принципи Трансферу:

- Згода особи, яку дані стосуються
- Виконання договору
- Виконання законодавчих обов'язків
- Захист даних під час трансферу

Організації можуть використовувати сертифікаційні програми для забезпечення захисту даних під час міжнародного трансферу.

Механізми Міжнародного Трансферу. Організації можуть використовувати стандартні контрактні клаузули, затверджені регуляторними органами, для забезпечення захисту даних під час трансферу.

Організації можуть розробити біндінгові корпоративні правила для забезпечення захисту даних під час трансферу між філіями.

Організації повинні гарантувати, щоб країна, до якої передаються дані, забезпечувала адекватний рівень захисту даних.

Відповідальність за Міжнародний Трансфер. Організація, яка експортує дані, несе відповідальність за забезпечення захисту даних під час трансферу.

Організація, яка імпортує дані, несе відповідальність за дотримання законодавства про захист даних у своїй країні.

Суперечки та спори при міжнародному трансфері. Механізми вирішення суперечок: Міжнародний арбітраж. Судові процедури. Медіація та інші альтернативні методи вирішення спорів.

Юрисдикція та правове регулювання: Визначення юрисдикції у разі суперечок. Застосування законодавства про захист даних у країнах-учасницях трансферу.

Захист прав осіб, яких дані стосуються: Інформування осіб про трансфер даних та потенційні ризики. Захист прав осіб у разі порушення законодавства про захист даних.

Нові тенденції та виклики у міжнародному трансфері

Інформаційні технології та клауд-комп'ютинг: Виклики щодо захисту даних у хмарі. Переваги використання місцевих центрів обробки даних.

Штучний інтелект та автоматизація: Ризики щодо біометричних даних та профайлінгу. Потреба у прозорості та пояснюваності процесів штучного інтелекту.

Глобальна гармонізація законодавства про захист даних: Ініціативи щодо створення єдиних стандартів захисту даних. Переваги та виклики глобальної гармонізації законодавства.

Додаток А: Перелік використаних абревіатур та термінів

Абревіатури:

GDPR - Регламент ЄС про захист даних

CCPA - Каліфорнійський закон про конфіденційність споживачів

ISO 27001 - Міжнародний стандарт інформаційної безпеки

Терміни:

Персональні дані

Обробка даних

Конфіденційність даних

Безпека даних

Додаток Б: Зразок політики захисту персональних даних

Структура Політики:

- Вступ
- Правила обробки персональних даних
- Міри безпеки даних
- Процедури реагування на інциденти
- Оновлення політики

Приклади Політики:

Зразок заяви про конфіденційність

Зразок інформованої згоди на обробку даних

Зразок Заяви про Конфіденційність

Назва Організації: Український Онлайн-Сервіс **Дата Останнього Оновлення:** 01 лютого 2025 року

Заява про Конфіденційність

Український Онлайн-Сервіс серйозно ставиться до захисту Вашої конфіденційності. Ця заява про конфіденційність пояснює, як ми збираємо, використовуємо та захищаємо Ваші персональні дані під час використання нашого веб-сайту та послуг.

Що ми збираємо:

Персональні дані: Ім'я, прізвище, адресу електронної пошти, номер телефону (при реєстрації або замовленні послуг)

Інформація про використання: Історія відвідувань, IP-адреса, тип браузера та операційної системи (для покращення роботи сайту)

Як ми використовуємо зібрані дані:

- Проведення реєстрації та авторизації
- Надання замовлених послуг та підтримка
- Покращення роботи сайту та послуг
- Надсилання інформаційних матеріалів (якщо Ви погодилися на це)

Як ми захищаємо Ваші дані:

- Шифрування даних під час передачі (HTTPS)
- Безпека серверів та інфраструктури
- Обмежений доступ до даних лише для авторизованих осіб

Ваші Права:

- Доступ до своїх персональних даних
- Виправлення чи видалення даних
- Відмова від обробки даних для маркетингових цілей
- Представлення скарги регуляторним органам

Зміни у Заяві про Конфіденційність:

Ми повідомимо Вас про будь-які суттєві зміни цієї заяви про конфіденційність на цій сторінці. Останнє оновлення: 01 лютого 2025 року.

Контакти:

Для питань щодо цієї заяви про конфіденційність чи Вашої конфіденційності, будь ласка, звертайтесь: зворотній адрес електронної пошти +380 (XX) XXX-XX-XX

Зразок інформованої згоди на обробку даних

Форма інформованої згоди

Назва організації: Український Онлайн-Сервіс

Мета обробки даних: Реалізація реєстрації та надання замовлених послуг на нашому веб-сайті.

Категорії персональних даних, які будуть оброблені:

Ім'я та прізвище

Адреса електронної пошти

Номер телефону

Право на відмову: Ви маєте право відмовитися від обробки даних для маркетингових цілей в будь-який час, надіславши нам повідомлення на зворотній адрес електронної пошти.

Термін зберігання даних: Дані будуть зберігатися протягом терміну надання послуг чи до моменту Вашої відмови від обробки даних, залежно від того, що відбувається раніше.

Захист даних: Ми застосовуємо заходи безпеки для захисту Ваших даних, зокрема шифрування даних під час передачі (HTTPS) та обмежений доступ до даних.

Представлення скарги: Ви маєте право подати скаргу регуляторним органам, якщо вважаєте, що обробка您的 даних порушує законодавство про захист даних.

Погодження:

Я, [**Ваше Ім'я та Прізвище**], повідомлений(а) про мету, умови та ризики обробки моїх персональних даних Українським Онлайн-Сервісом, погоджуюсь з обробкою моїх даних для реєстрації та надання послуг на умовах, зазначених вище.

Дата: _____ **Підпис:** _____ (для друку) / Чекбокс згоди (для онлайн-форм)

Тема 3. Складання та перевірка електронних договорів

1. Створити проект «КОНТРАКТ». Визначити ролі, етапи виконання, створити таблиці відповідальності та термінів виконання.
2. Використати штучний інтелекту для створення тексту контракту.
3. Оформити контракт у Microsoft Word або Google Doc із використанням стилів, коментарів і функцій співпраці
4. Підписати контракт ЕЦП.
5. Використти інтернет-сервіси для аналізу контракту

Тема 4. Організація та налаштування електронного документообігу

Перевірити можливості цифрових он-лайн інструментів :

- **ONLYOFFICE Personal** для редагування та зберігання документів із підтримкою спільної роботи;
- **DocHub** – для підписання та перевірки документів.

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: електронний документ, система електронного документообігу.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

Електронний документообіг являє собою процес створення, зберігання, передачі та управління електронними документами у різних сферах діяльності, включно з юридичною практикою. Це поняття охоплює широкий спектр дій, спрямованих на оптимізацію роботи з документами шляхом використання інформаційних технологій.

У юридичній практиці електронний документообіг набуває особливого значення, оскільки дозволяє скоротити час обробки документів, зменшити витрати на папір та архівування, а також підвищити рівень безпеки та конфіденційності документів.

Окремим аспектом електронного документообігу є використання спеціалізованих систем управління документами (EDMS), які забезпечують структурований підхід до створення, зберігання та пошуку документів.

Історія електронного документообігу тісно пов'язана з розвитком інформаційних технологій. Перші системи управління документами з'явилися у 1980-ті роки, проте справжній зліт електронного документообігу відбувся з початку 2000-х років, з поширенням широкосмугового інтернету та розвитку хмарних технологій.

Українське законодавство також пристосовується до вимог часу. У 2003 році був прийнятий Закон України "Про електронний документ та електронний документообіг", який встановлює основні принципи та вимоги до електронних документів та їх обігу.

Сучасний етап розвитку електронного документообігу характеризується інтеграцією штучного інтелекту, блокчейну та інших інноваційних технологій для підвищення безпеки, ефективності та прозорості документів.

Однією з найважливіших переваг електронного документообігу є значне скорочення часу обробки документів. Автоматизовані системи дозволяють швидко створювати, відправляти та обробляти документи, що підвищує продуктивність роботи організації.

Електронний документообіг також має екологічні переваги, оскільки зменшує потребу в папері та знижує вплив на навколишнє середовище. Крім того, електронні документи займають значно менше фізичного простору для зберігання.

Використання електронного документообігу також підвищує рівень безпеки документів завдяки застосуванню шифрування, цифрових підписів та інших засобів захисту. Це особливо важливо для юридичної практики, де конфіденційність документів є критичною.

Законодавчі основи електронного документообігу в Україні встановлені Законом України "Про електронний документ та електронний документообіг" від 2003 року. Цей закон визначає поняття електронного документа, встановлює вимоги до його створення, зберігання та передачі, а також регулює питання юридичної сили електронних документів.

Крім цього, інші нормативні акти, такі як Кодекс адміністративного судочинства України, Цивільний кодекс України та інші, містять окремі положення, що стосуються використання електронних документів у різних галузях права.

Законодавство України також відповідає міжнародним стандартам у сфері електронного документообігу, забезпечуючи взаємодію з іншими країнами у цій сфері.

Юридична сила електронних документів в Україні визначається їх відповідністю встановленим вимогам. Електронний документ має містити необхідну інформацію, бути підписаним електронним підписом та відповідати технічним вимогам, встановленим законодавством.

Електронний підпис є ключовим елементом, що підтверджує автентичність та цілісність електронного документа. Законодавство України встановлює різні види електронних підписів, серед яких кваліфікований електронний підпис володіє найбільш високим рівнем довіри.

Відповідно до законодавства, електронні документи мають таку саму юридичну силу, як і їх паперові аналоги, якщо вони відповідають встановленим вимогам.

За порушення правил електронного документообігу можуть бути застосовані різні види відповідальності. Адміністративна відповідальність передбачає накладення штрафів за порушення вимог до створення, зберігання та передачі електронних документів.

Цивільна відповідальність може бути застосована у випадку порушення прав осіб, пов'язаних з електронним документообігом, наприклад, через порушення конфіденційності або втрату даних.

Крім того, у разі тяжких порушень можуть бути застосовані кримінально-правові санкції, особливо якщо порушення пов'язані з умисним знищенням, пошкодженням або неприпустимим доступом до електронних документів.

У разі порушення вимог електронного документообігу, особи, відповідальні за ці порушення, можуть бути притягнуті до дисциплінарної відповідальності, яка може включати в себе попередження, догану, звільнення з посаді тощо.

Крім того, організації, що порушують правила електронного документообігу, можуть бути піддані публічній критиці, що може негативно вплинути на їх репутацію та довіру клієнтів.

Безпека електронних документів у юридичній практиці базується на трьох основних принципах: конфіденційності, цілісності та доступності. Конфіденційність забезпечується шляхом захисту документів від несанкціонованого доступу.

Цілісність гарантує, що документи не будуть змінені під час передачі або зберігання. Доступність забезпечує можливість швидкого доступу до документів для авторизованих осіб.

Для забезпечення безпеки електронних документів використовуються різні механізми захисту, серед яких:

Шифрування даних, яке перетворює інформацію в недоступний для несанкціонованого доступу формат. Цифрові підписи, що підтверджують автентичність та цілісність документів. Системи контролю доступу, які обмежують доступ до документів лише для авторизованих осіб. Резервне копіювання даних, яке забезпечує відновлення документів у разі їх втрати або пошкодження.

Юридичні компанії та організації повинні розробити та реалізувати ефективну політику безпеки електронних документів, яка включає:

Проведення регулярних аудитів безпеки інформаційних систем. Проведення навчальних програм для працівників щодо безпеки електронних документів. Створення системи швидкого реагування на інциденти безпеки.

У майбутньому електронний документообіг у юридичній практиці очікує значний розвиток, обумовлений зростанням використання штучного інтелекту, блокчейну та інших інноваційних технологій.

Ці технології відкривають нові можливості для підвищення ефективності, безпеки та прозорості документів, що може призвести до значної зміни юридичної практики.

Відповідно до розвитку технологій, юридична практика стоїть перед новими викликами, серед яких:

Необхідність постійного оновлення знань працівників щодо нових технологій. Потрібність адаптації законодавчої бази до вимог сучасного електронного документообігу. Зростання ризиків кібербезпеки та необхідність їх мінімізації.

Електронний документообіг у юридичній практиці є необхідним інструментом для підвищення ефективності та безпеки роботи з документами. Розуміння законодавчих аспектів, механізмів захисту та перспектив розвитку цього напрямку є ключовим для успішної реалізації електронного документообігу в юридичних організаціях.

Тема 5. CRM-системи та їх роль у юридичному бізнесі

1. Створити п’ять карток з інформацією про клієнта для подальшого формування бази CPM-системи
2. Розробити перелік (рейтинг) чинників впливу на формування воронки продаж CPM-системи

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: формуванн клієнтської бази, управління контрактами, управління документами, сценарій взаємодії.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

CRM (Customer Relationship Management) система – це комплексна технологічна платформа, призначена для управління взаєминами з клієнтами та оптимізації бізнес-процесів компанії.

У юридичному бізнесі, CRM системи допомагають керувати спілкуванням з клієнтами, відстежувати справи та підвищувати ефективність роботи юридичної команди.

Основною метою впровадження CRM системи є поліпшення клієнтського досвіду та збільшення прибутків компанії через більш ефективне управління відносинами з клієнтами.

1. Основні функції CRM системи: **Управління контактами:** Центральна база даних для зберігання інформації про клієнтів, включаючи контактні дані, історію взаємин та особисті преференції. Автоматизація процесу оновлення контактної інформації для забезпечення точності та актуальності даних. Можливість доступу до інформації про клієнтів для всіх членів команди в режимі реального часу. **Управління справами та проектами:** Інструменти для створення, призначення та відстеження справ та проектів, включаючи встановлення термінів виконання та призначення відповідальності. Візуалізація прогресу справ за допомогою діаграм Ганта або календарів для покращення планування. Автоматизація звітності для ефективного моніторингу стану справ.

2. Роль CRM системи в управлінні клієнтами в юридичному бізнесі: Поліпшення клієнтського досвіду: CRM системи дозволяють юридичним компаніям забезпечити персоналізований підхід до клієнтів, беручи до уваги їхні індивідуальні потреби та очікування. Систематизація комунікацій з клієнтами допомагає уникнути втрати важливої

інформації та забезпечити своєчасну реакцію на запитання та проблеми клієнтів. Збільшення клієнтської лояльності завдяки покращенню рівня задоволеності клієнтів послугами компанії. ***Підвищення ефективності юридичної команди:*** Автоматизація рутинних завдань звільняє час юридичної команди для фокусу на стратегічних та пріоритетних завданнях. Покращення співпраці між членами команди шляхом забезпечення спільного доступу до інформації про клієнтів та справи. Оцінка ефективності роботи юридичної команди та ідентифікація областей для покращення за допомогою аналітичних інструментів CRM.

3. Вибір та впровадження CRM системи для юридичного бізнесу. Критерії вибору CRM системи: **Функціональність та гнучкість:** Спроможність системи відповідати конкретним потребам юридичної компанії, включаючи управління справами та контактами. Можливість налаштування системи відповідно до внутрішніх процесів компанії. Інтеграція з існуючим програмним забезпеченням (наприклад, електронна пошта, бухгалтерське програмне забезпечення). **Безпека та конфіденційність:** Високий рівень захисту даних клієнтів та компанії від несанкціонованого доступу. Сумісність з нормативними вимогами щодо захисту даних (наприклад, GDPR, CCPA). Регулярне оновлення системи для захисту від нових загроз. **Процес впровадження CRM системи:** Планування та підготовка: визначення цілей впровадження, формування команди проекту та розробка плану впровадження. Налаштування та інтеграція: встановлення системи, налаштування функцій відповідно до потреб компанії та інтеграція з існуючим програмним забезпеченням. Тренінг та підтримка: навчання користувачів, забезпечення технічної підтримки та постійного моніторингу ефективності системи.

CRM система є потужним інструментом для юридичних компаній, який допомагає покращити управління відносинами з клієнтами, підвищити ефективність роботи команди та збільшити прибуток.

Вибір правильної CRM системи, яка відповідає конкретним потребам компанії, є критичним для успішного впровадження.

Постійний моніторинг та оновлення системи забезпечують її ефективність у динамічному бізнес-середовищі.

Тема 6. Кіберзлочинність та правове регулювання

1. Створити рекомендації по використанню **Онлайн-ресурсів**:

- **CyberChef** для аналізу даних і форматуванню інформації;
- **Kali Linux (з базовими інструментами)** для аналізу кіберзагроз;
- **PhishTank** для перевірки підозрілих посилань;
- **Google Transparency Report** для отримання інформації про небезпечні веб-сайти.

2. У матеріалах новин за останній місяць по телебаченню та в мережі Інтернет відшукати різні види інформаційного психологічного впливу (інформаційного маніпулювання, фейків, пропаганди, дезінформації тощо).

3. Отриману інформацію структурувати та розмістити у таблиці

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: кіберзлочини, фішінг, хакінг,смарт-контракт,

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

Кіберзлочинність - це злочинна діяльність, що здійснюється шляхом використання інформаційно-комунікаційних технологій (ІКТ), зокрема Інтернету, для досягнення незаконних цілей. Це може включати порушення конфіденційності, цілісності або доступності інформаційних активів.

Кіберзлочинність часто здійснюється за допомогою спеціалізованого програмного забезпечення та технік, які дозволяють злочинцям залишатися анонімними. Це створює суттєві проблеми для правоохоронних органів під час розслідування та переслідування злочинців.

Визначення кіберзлочинності постійно еволюціонує, оскільки злочинці адаптуються до нових технологій та методів захисту. Тому законодавство та правоохоронна практика повинні бути гнучкими, щоб ефективно протидіяти цим злочинам.

Класифікація кіберзлочинності:

Кіберзлочини проти осіб:

Ця категорія включає злочини, спрямовані проти окремих осіб, такі як кіберсталкінг, сексуальне насильство в Інтернеті та кібербулінг. Ці злочини можуть мати серйозні психологічні та емоційні наслідки для потерпілих.

Кіберзлочини проти осіб часто здійснюються через соціальні мережі, електронну пошту або інші онлайн-платформи. Злочинці можуть використовувати персональну інформацію, щоб завдати більший збиток.

Правове регулювання цих злочинів повинно забезпечувати ефективну захист жертв та передбачати суворі покарання для злочинців, одночасно гарантуючи дотримання прав людини.

***Кіберзлочини проти власності*:** Хакінг; Фішинг; Підробка програмного забезпечення

Кіберзлочини проти державної безпеки: Кібершпигунство; Кібертероризм; Порушення інформаційної безпеки держави

Правове Регулювання Кіберзлочинності

Міжнародне Правове Регулювання:

Конвенція про кіберзлочинність (Будапешт, 2001) є ключовим міжнародним документом, який встановлює стандарти для країн щодо боротьби з кіберзлочинністю. Вона охоплює широкий спектр аспектів, від хакінгу до захисту даних.

Резолюції ООН щодо кібербезпеки підкреслюють важливість міжнародної співпраці у сфері протидії кіберзлочинності та конфліктів. Вони закликають держави зміцнювати свої законодавчі бази та співпрацювати у сфері кібербезпеки.

Реалізація цих міжнародних угод часто вимагає від країн адаптувати своє національне законодавство, щоб відповідати встановленим стандартам, що може бути складним процесом, особливо для країн з обмеженими ресурсами.

Національне правове регулювання:

Кримінальний Кодекс України (статті 361-363):

Ці статті встановлюють відповідальність за кіберзлочини, зокрема за несанкціонований доступ до інформаційних систем, порушення єдиності та цілісності програмного забезпечення тощо.

Законодавство України спрямоване на забезпечення захисту інформації та інформаційно-телекомунікаційних систем від незаконних впливів.

Практика застосування цих статей показує, що ефективна боротьба з кіберзлочинністю вимагає не лише законодавчих заходів, але й підвищення обізнаності населення та спеціальної підготовки правоохоронців.

Інструменти Боротьби з Кіберзлочинністю

Технічні інструменти:

Системи виявлення та запобігання вторгненню (IDS/IPS) є критичними для захисту мереж та систем від кібератак. Вони можуть автоматично виявляти та блокувати підозрілу діяльність.

Антивірусне програмне забезпечення допомагає захистити комп'ютери та мережі від шкідливого програмного забезпечення (малвару), яке часто використовується злочинцями для доступу до систем.

Технології шифрування забезпечують конфіденційність даних, навіть якщо вони будуть перехоплені злочинцями, зробивши їх недоступними для використання.

Правові інструменти:

Судові процеси проти кіберзлочинців є кінцевим етапом боротьби з цими злочинами. Вони забезпечують відповідальність злочинців та дієвий засіб запобігання майбутнім злочинам.

Міжнародна співпраця у сфері кібербезпеки є життєво необхідною для ефективної боротьби з транснаціональними кіберзлочинами.

Освіта та підвищення обізнаності населення про кібербезпеку допомагають запобігати кіберзлочинам, надаючи людям знання про безпечну поведінку в Інтернеті.

Сучасні тенденції та виклики у сфері кіберзлочинності.

Розвиток смарт-контрактів та кібербезпека:

Смарт-контракти, засновані на блокчейн-технології, пропонують підвищену безпеку та прозорість транзакцій, але також створюють нові виклики щодо захисту від кібератак.

Переваги використання смарт-контрактів включають автоматизацію процесів та зниження ризику фальсифікації, проте вони вимагають спеціалізованих заходів кібербезпеки.

Необхідність розвитку спеціалізованих законодавчих рамок для регулювання смарт-контрактів та забезпечення їхньої безпеки є однією з ключових сучасних тенденцій.

Кіберзлочинність у добу штучного інтелекту:

Злочинці все частіше використовують штучний інтелект (ШІ) для здійснення складніших та більш підступних кібератак.

Розробка ШІ-засобів для протидії кіберзлочинності стає все більш важливою, оскільки ці технології можуть допомогти виявляти та зупиняти атаки більш ефективно.

Питання етичного використання ШІ у сфері кібербезпеки та протидії злочинам залишається відкритим для дискусій та подальшого дослідження.

Однією з найбільших проблем є використання ШІ для створення реалістичних фішингових повідомлень або для проведення складних соціальних інженерних атак.

Розробка ефективних засобів захисту проти ШІ-підтримуваних кібератак вимагає значних інвестицій у дослідження та розвиток нових технологій безпеки.

Міжнародна співпраця у сфері розробки стандартів безпеки для ШІ-систем стає все більш важливою для протидії транснаціональним кіберзлочинам.

Глобальна співпраця у сфері кібербезпеки:

Глобальна співпраця між країнами, організаціями та приватним сектором є ключовим елементом ефективної боротьби з кіберзлочинністю.

Ініціативи, такі як створення спільних центрів реагування на інциденти кібербезпеки, допомагають підвищити рівень підготовки до кібератак.

Гармонизація законодавчих рамок щодо кібербезпеки між країнами полегшує проведення спільних розслідувань та покарання злочинців.

Майбутнє кібербезпеки та боротьби з кіберзлочинністю

Технологічні інновації у сфері кібербезпеки:

Розробка та впровадження нових технологій, таких як квантовий комп'ютер та покращені системи штучного інтелекту, можуть революціонізувати сферу кібербезпеки.

Використання блокчейн-технологій для підвищення безпеки даних та транзакцій вже показало свою ефективність у багатьох галузях.

Необхідність постійного оновлення знань та навичок фахівців кібербезпеки для роботи з новими технологіями є однією з ключових майбутніх тенденцій.

Правові системи світу будуть продовжувати адаптуватися до нових кіберзлочинних загроз, розробляючи більш ефективне та гнучке законодавство.

Міжнародна співпраця у сфері розвитку правових рамок для нових технологій, таких як ШІ та блокчейн, буде відігравати все більш важливу роль.

Гарантія дотримання прав людини в умовах розвитку технологій спостереження та контролю стане однією з найбільших правових та етичних викликів майбутнього.

Кіберзлочинність є динамічною та постійно еволюціонуючою загрозою, яка вимагає гнучкої та ефективної реакції зі сторони законодавства, правоохоронних органів та суспільства в цілому.

Підвищення обізнаності про кібербезпеку, розвиток спеціалізованих законодавчих рамок та міжнародна співпраця є ключовими елементами успішної боротьби з кіберзлочинністю.

Майбутнє кібербезпеки залежить від нашої здатності адаптуватися до нових технологій та загроз, зберігаючи при цьому баланс між безпекою та правами людини.

Тема 7. Електронне судочинство

1. Розробити відеоінструкції для клієнтів щодо подання електронних документів через «Електронний суд».
2. Розробити інфографіку, що пояснює структуру договору або судового процесу.
3. Скласти схему модулів ЄСІТС та взаємодію між елементами.
4. Визначити за допомогою сайту «Судова влада України», чи розглядаються і де саме справи, де сторони мають прізвище здобувача вищої освіти (з уточненням суду, категорії справи), які справи призначені до розгляду у відповідному місцевому суді в день проведення практичного заняття.

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: ЄСІТС, Електронний суд.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

Комп'ютеризація судів сьогодні є стратегічним напрямом підвищення оперативності судочинства. У зв'язку зі змінами соціально-економічної ситуації в країні, зростанням злочинності, збільшенням і якісною зміною змісту цивільних справ, розширенням можливостей оскарження у суді неправомірних дій посадових осіб навантаження на органи судової влади зростає з кожним роком.

Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) — організаційно-технічна система, що забезпечує функціонування електронного судочинства в Україні. До функцій цієї системи відноситься, зокрема, ведення електронного діловодства, зберігання документів та інформації в єдиній базі даних, захищене зберігання справ в електронному архіві; обмін документами та інформацією в електронній формі, проведення відеоконференцій, формування і ведення суддівського досьє, віддалений доступ користувачів до будь-якої інформації у системі, ведення Єдиного державного реєстру судових рішень, функціонування офіційного веб-порталу судової влади України, веб-сайтів Вищої ради правосуддя та Вищої кваліфікаційної комісії суддів України, функціонування єдиного контакт-центру для управління зверненнями та ін.

Тема 8. Цифрові інструменти в юридичній практиці

1. Розв'язання юридичних задач засобами ІППС. Правове обґрунтування пунктів контракту.
2. Знайомство та основні прийоми роботи з сучасною онлайн-платформою для юриста ***ActiveLex***
3. Мова запитів, пошук документів. Зв'язки. Формування портфеля у ***ActiveLe***

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: аналіз юридичних даних, автоматизація процесу управління справати, машинне навчання, штучний інтелект

***З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах*:**

Цифрові інструменти в юридичній практиці - це програмне забезпечення, платформи та технології, які застосовуються для підвищення ефективності, продуктивності та якості юридичних послуг. Вони охоплюють широкий спектр застосунків, від управління справами та документів до аналізу даних та штучного інтелекту. Ці інструменти допомагають юристам, адвокатам та юридичним компаніям адаптуватися до сучасного цифрового середовища.

1. **Основні види цифрових інструментів:**

- Системи управління справами (Case Management Systems): Автоматизація процесу управління справами, включаючи призначення завдань, відстеження прогресу та звітність. Інтеграція з іншими інструментами для комплексного управління юридичними процесами.
- Платформи електронного обміну документообігу. Безпечний та контрольований обмін документами між сторонами, включаючи підписання електронних документів. Зниження ризику втрати або порушення конфіденційності документів.
- Інструменти аналізу юридичних даних (Legal Data Analytics Tools): Використання даних для прийняття інформованих рішень, включаючи аналіз судових рішень, законодавчих змін та ринку юридичних послуг. Покращення стратегічного планування та підвищення ефективності юридичної роботи.

Переваги цифрових інструментів: Покращення продуктивності: Автоматизація рутинних завдань звільняє час для стратегічної роботи. Підвищення якості служб: Доступ до актуальної інформації та інструментів аналізу покращує якість юридичних консультацій. Зниження витрат: Оптимізація процесів та зменшення потреби в паперовій документації.

Виклики та обмеження: Безпека та конфіденційність: Захист інформації від несанкціонованого доступу. Технічні вимоги та навчання: Необхідність технічних знань та інвестицій у навчання персоналу. Єднання з традиційними підходами: Інтеграція цифрових інструментів у існуючі бізнес-процеси та культуру компанії.

2. **Майбутнє цифрових інструментів в юридичній практиці:**

- Тенденції та інновації: Штучний інтелект (AI) та машинне навчання: Автоматизація складних завдань, передбачення результатів справ та персоналізація юридичних послуг. Блокчейн та безпечний обмін даними: Покращення безпеки та прозорості юридичних транзакцій. Хмарні технології: Гнучкість, масштабованість та доступність юридичних інструментів через Інтернет.
- Стратегії адаптації до змін: Моніторинг ринку: Постійне спостереження за новими технологіями та тенденціями. Інвестиції у розробку персоналу: Підтримка технічних та інформаційних компетенцій працівників. Гнучка бізнес-стратегія: Готовність до швидкої адаптації бізнес-моделі у відповідь на зміни ринку.

Цифрові інструменти революціонізують юридичну практику, пропонуючи нові можливості для підвищення ефективності, якості та інноваційності юридичних послуг. Юридичні компанії, які успішно адаптуються до цих змін, матимуть конкурентну перевагу на ринку. Постійне навчання, інновації та гнучкість будуть ключовими для майбутнього успіху в юридичній сфері.

Веб-ресурси Верховної Ради України є офіційним джерелом інформації Верховної Ради України, що забезпечують висвітлення діяльності Верховної Ради України, парламентських органів та Апарату Верховної Ради України, сприяють обміну інформацією з іншими органами державної влади та органами місцевого самоврядування, інформаційній взаємодії з урядовими і неурядовими організаціями інших країн, із громадськістю.

Веб-ресурси Верховної Ради України поділяються за призначенням:

- для користувачів глобальної мережі Інтернет;
- для користувачів локальної мережі Верховної Ради України Інтернет.

ЛІГА:ЗАКОН — інформаційно-правова і комунікаційна платформа для бізнесу. ЛІГА: ЗАКОН стояла біля витоків появи і розвитку в Україні такого явища як комп'ютеризовані правові бази даних. З моменту своєї появи в 1991 році і до сьогоднішнього дня основним завданням ЛІГА: ЗАКОН є розвиток правових систем, які дозволяли б вирішувати широкий спектр правових питань, що виникають в роботі як юристів і бухгалтерів, так і керівників компаній.

Окрім, власне законодавчої бази, платформа дає можливість доступу до аналітичної та консультаційної інформації. Зокрема, мова йде про такі інформаційно-правові системи для юриста, як «Законодавство України», «Правова картина дня», «Термінологічний словник», «Календар юриста» «Законопроекти», «Ситуації для юриста», «Судова практика», «Коментовані кодекси», «Європейське законодавство», «Мистецтво оборони», «Судові прецеденти», «Калькулятор штрафів».

Тема 9. Мультимедійна підтримка юридичної діяльності

1. Підготувати плану вебінару для клієнтів щодо захисту прав споживачів із використанням , GoogleMeet, або Microsoft Teams.

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: медіа-формат, інтерактивні інструменти, візуалізація інформації

***З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах*:**

- Використання різних медіа-форматів (текст, зображення, аудіо, відео, анімація) для забезпечення ефективної комунікації, документування та аналізу юридичної інформації.
- Інтеграція мультимедійних інструментів у юридичні процеси для покращення якості послуг та підвищення клієнтського досвіду.

Основні види мультимедійної підтримки: Відеоконференції та онлайн-спори:

- Використання відео зв'язку для проведення судових засідань, переговорів та консультацій на відстані. Забезпечення інтерактивності та візуальної комунікації для більш ефективного спілкування.
- Інтерактивні презентації та візуалізація даних: Створення інтерактивних презентацій для пояснення складних юридичних концепцій клієнтам. Використання візуалізації даних для аналізу та представлення великих обсягів юридичної інформації. Аудіо- та відеозаписи судових розглядів: Запис судових засідань для документації та подальшого аналізу. Використання транскрипційних технологій для створення текстових версій аудіо-/відеозаписів.

2. Інструменти та технології мультимедійної підтримки

- Інструменти для відеоконференцій:
  - Zoom
  - Skype
  - Google Meet
- Інструменти для Інтерактивних Презентацій:
  - PowerPoint
  - Prezi
  - Google Slides
- Інструменти для візуалізації даних:
  - Tableau
  - Power BI
  - D3.js

- Технології аудіо-/відеозапису та транскрипції:
  - Digital Voice Recorders
  - Screen Recording Software
  - Automatic Speech Recognition (ASR) Технології

Переваги Мультимедійної Підтримки: Покращення комунікації: Ефективніше спілкування між юристами, клієнтами та судовими органами. Збільшення продуктивності: Автоматизація документів та процесів для зменшення адміністративного навантаження. Підвищення якості служб: Індивідуалізовані підходи до клієнтів завдяки інтерактивним інструментам.

Виклики та Обмеження: Безпека та конфіденційність: Захист чутливої інформації від несанкціонованого доступу. Технічні вимоги та навчання: Необхідність технічних знань та інвестицій у навчання персоналу. Сумісність з судовими процедурами: Виконання вимог судової системи щодо документів та процедур.

Мультимедійна підтримка юридичної діяльності відкриває нові можливості для покращення якості послуг, підвищення ефективності та задоволення клієнтів.

Для успішної реалізації мультимедійних інструментів необхідно вирішити технічні, юридичні та соціальні питання.

Постійний розвиток та адаптація технологій будуть ключовими для майбутнього розвитку юридичної діяльності.

1.5. Індивідуальні завдання

1.5.1.Основні вимоги до написання індивідуальних завдань

Індивідуальні завдання передбачаються у формі виконання індивідуальних або колективних проєктів. Можуть виконуватися науково-дослідні завдання за освітнім компонентом.

Завдання у формі ІНДЗ обирається студентом добровільно на початку семестру без повторів. Виконання індивідуального завдання у формі ІНДЗ передбачає створення аналітичного огляду з підготовкою текстового документа та презентації ІНДЗ на практичних заняттях (виступ до 5 хвилин).

Роботи представляються в електронній формі та повинні відповідати вимогам оригінальності, самостійності та дотримання правил академічної доброчесності.

Методичні вказівки

При вивченні даної теми студенту слід розуміти такі ключові поняття і категорії, як: інформація, особливості ІКТ для правничої діяльності, відкриті та персональні дані, діджиталізація.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

Загальний обсяг роботи – 5–8 сторінок друкованого тексту. Робота повинна бути написана державною мовою. Робота починається з титульного аркуша, оформленого згідно з чинними нормами. На другій сторінці роботи розташовують “ЗМІСТ”. У ньому наводяться назви всіх структурних частин роботи з початковим номером сторінки, на якій розділ починається. Усі структурні розділі роботи нумеруються арабськими цифрами (окрім “ВСТУПУ”, “ВИСНОВКІВ”, “СПИСКУ ЛІТЕРАТУРИ”) та друкуються великими літерами. Розділи та підрозділи роботи повинні бути відокремлені збільшеним міжрядковим інтервалом. У кінці заголовків крапка не ставиться.

Сторінки нумерують у верхньому правому куті сторінки. На титульному аркуші номер не ставиться, але він входить до загальної кількості сторінок. Нумерацію сторінок починають із “ЗМІСТУ” – “2. Нумерацію сторінок закінчують на останній сторінці “списку літератури”. Береги (поля) на сторінці повинні складати відповідно: верхній – 20 мм, нижній – 20, зліва –

30, справа – 15 мм. Рекомендовані параметри друку: шрифт Times New Roman, розмір літер 14, міжрядковий інтервал –1,0–1,2.

Об'єм вступу не повинен перевищувати 1 сторінки. Вступ (умовно) складається із трьох частин. У першій характеризується досліджуваний об'єкт (явище), доводиться актуальність обраної теми. Друга частина вступу висвітлює загальний стан вивченості об'єкту досліджень та підводить до заключної третьої частини вступу – мети роботи (1 речення) та її завдань (2–4 пункти).

Розділ повинен бути побудований таким чином, щоб при читанні тільки вступу й висновків у стороннього читача склалося повне уявлення про те, що досліджувалося в роботі й навіщо.

Обсяг висновків не повинен перевищувати 1 сторінки. Висновки зазвичай складаються із 3–7 пунктів. До складу кожного пункту входить 1–3 речення.

"СПИСОК ЛІТЕРАТУРИ" або "ЛІТЕРАТУРА" подаються за одним із двох принципів. Рекомендована кількість джерел складає 15–20. Усі джерела, наведені в цьому розділі повинні бути проаналізовані в тексті роботи (не повинно бути зайвих джерел). І навпаки, всі джерела, на які є посилання в тексті роботи, повинні бути зазначені у "СПИСКУ ЛІТЕРАТУРИ".

Заголовки структурних частин друкуються великими літерами симетрично до тексту. Заголовки підрозділів – маленькими літерами (крім першої літери) з абзацного відступу. Якщо заголовок складається з двох або більше речень, їх розділяють крапкою. Відстань між заголовками (за винятком заголовка пункту) та текстом повинна дорівнювати 3–6 пт.

Ілюстрації, рисунки, схеми, графіки, таблиці необхідно подавати безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці. Ілюстрації позначають словом "Рис." та нумерують послідовно за винятком ілюстрацій, поданих у додатках. Таблиці нумерують послідовно в межах кожного розділу. У правому верхньому куті над заголовком таблиці розміщують напис "Таблиця" їх зазначенням її номера. При переносі частини таблиці на інший аркуш вказують "Продовження табл. 1.2." Номер формул пишуть по правому полю аркуша на рівні відповідної формули в круглих дужках.

Список літератури необхідно наводити в алфавітному порядку (спочатку україномовні джерела, потім – іншомовні).

Аналітичний огляд. Індивідуальні навчально-дослідні завдання.

Структура ІНДЗ:

- зміст;
- вступ – обґрунтовується тема, мета та завдання роботи;
- основні результати роботи та їх обговорення – подаються у лаконічній формі, схематизованому вигляді, найчастіше поділяються на 3–4 розділи залежно від змісту конкретної теми; бажано розділи також структурувати на 2–4 підрозділи, обсягом по декілька абзаців;
- висновки;
- список використаної літератури.

1.5.1. Тематика індивідуальних завдань

1. Еволюція інформаційно-комунікаційних технологій у правовій сфері: від паперового документообігу до цифрової ери.
2. Основні виклики та перспективи цифровізації юридичної діяльності.
3. Вплив ІКТ на трансформацію юридичних послуг та взаємодію з клієнтами.
4. Порівняльний аналіз цифрової зрілості правничих систем у різних країнах.

5. Розвиток електронного судочинства: міжнародний досвід та українські реалії.
6. Електронне подання процесуальних документів: правові та технічні аспекти.
7. Використання штучного інтелекту у судовій системі: автоматизований аналіз судової практики.
8. Перспективи впровадження блокчейн-технологій у судочинство.
9. Юридичні чат-боти: перспективи та обмеження їх використання в консультуванні.
10. CRM-системи для юридичних фірм: огляд найпопулярніших рішень.
11. Використання правових інформаційних систем у практиці юриста.
12. Big Data та аналітика у юридичній діяльності: інструменти для прогнозування судових рішень.
13. Основні виклики захисту персональних даних в епоху цифровізації.
14. Вплив регламенту GDPR на роботу юридичних фірм: аналіз основних положень.
15. Кіберзагрози для юридичного бізнесу: методи захисту та попередження атак.
16. Практичні аспекти впровадження політик інформаційної безпеки у юридичних фірмах.
17. Правові аспекти цифрового підпису та електронного документообігу.
18. Законодавче забезпечення правового статусу цифрових доказів у судочинстві.
19. Міжнародні стандарти регулювання цифрових правових послуг (GDPR, eIDAS).
20. Цифрові права людини: теоретичні підходи та практика їх реалізації.
21. Блокчейн у праві: можливості для зберігання та захисту даних.
22. Роль штучного інтелекту в автоматизації юридичних рутинних процесів.
23. Використання хмарних технологій у правничій діяльності: переваги та ризики.
24. Аналіз перспектив використання доповненої реальності у правовій освіті та практиці.
25. Переваги впровадження систем електронного документообігу у юридичних фірмах.
26. Аналіз ефективності роботи з платформами електронного документообігу (M.E.Doc, Вчасно, DealRoom).
27. Електронна комунікація між адвокатом і клієнтом: ризики та шляхи їх уникнення.
28. Етичні питання використання інформаційних технологій у правничій діяльності.
29. Вплив цифрових технологій на конфіденційність та адвокатську таємницю.
30. Особливості ведення юридичних справ у соціальних мережах та месенджерах

1.6. Підсумковий контроль

Підсумковий семестровий контроль проводиться у формі виконання тестових завдань.

1.6.1. Питання для підсумкового контролю

1. Основи цифровізації у правничій діяльності.
2. Значення впровадження ІКТ для підвищення ефективності роботи юристів.
3. Практичний аналіз переваг цифрових рішень, таких як автоматизація процесів, покращення комунікації та доступ до інформації.
4. Розгляд викликів, зокрема ризиків кібербезпеки та проблем адаптації нових технологій.
5. Законодавче регулювання використання ІКТ у правничій сфері в Україні.
6. Практичні завдання включають аналіз кейсів із впровадження ІКТ у юридичній діяльності та створення індивідуального плану цифровізації для юридичної фірми чи проєкту.
7. Використання відкритих реєстрів і баз даних (ЄДРПОУ, реєстри нерухомості тощо).
8. Методи збору, аналізу та візуалізації даних.
9. Практичні аспекти забезпечення захисту персональних даних у цифровому середовищі.

10. Оцінка політик конфіденційності сайтів чи додатків на відповідність вимогам українського законодавства та GDPR.

11. Використання інструментів для аналізу обробки та зберігання даних у бізнес-середовищі: Google Sheets, MS Excel, Power BI.

12. Практичні рекомендацій для забезпечення відповідності законодавству про захист персональних даних.

13. Створення політик конфіденційності для юридичних фірм або комерційних проектів.

14. Практичні аспекти ідентифікації ризиків, пов'язаних із обробкою даних, та їх мінімізації.

15. Автоматизовані платформи, що містять шаблони договорів.

16. Нормативні та практичні аспекти використання електронного підпису, його видів та особливостей застосування.

17. Типові ризики електронних угод і способи їх мінімізації

18. Використання Legal Tech платформ та штучного інтелекту для автоматизації процесів створення, перевірки та оптимізації юридичних документів.

19. Інструменти для перевірки відповідності та оцінки ризиків у договорах (AI-аналіз).

20. Практичні аспекти впровадження системи електронного документообігу (ЕДО) у юридичній фірмі.

21. Вибір програмного забезпечення для створення, зберігання та спільного редагування документів (наприклад, ВЧАСНО, SCHRIFT, M.E.Doc, Microsoft SharePoint, Google Workspace).

22. Оптимізація процесів підготовки, пошуку та передачі документів у цифровому середовищі.

23. Створення робочих процесів для команди, забезпечення доступу до документів із різними рівнями прав.

24. Інтеграція системи ЕДО з іншими інструментами управління бізнес-процесами, такими як CRM.

25. Створення та управління робочими процесами в юридичній фірмі.

26. Практичні аспекти налаштування ЕДО, включно з контролем версій документів та автоматизацією погоджень.

27. Основні переваги використання CRM-систем для юридичних фірм.

28. Типові ризики, пов'язані із впровадженням CRM-систем у юридичну практику, і способів їх подолання

29. Управління клієнтами та справами через CRM (Clio, KEY, СВОЯ).

30. Види кіберзлочинів і їх кваліфікація.

31. Регулювання кібербезпеки на національному та міжнародному рівнях.

32. Практичні аспекти забезпечення кібербезпеки у роботі юридичних фірм.

33. Методи захисту конфіденційної інформації та цифрових даних від несанкціонованого доступу.

34. Розробка політики кібербезпеки для юридичної організації: ідентифікація потенційних ризиків та створення плану реагування.

35. Практичні аспекти налаштування базових інструментів кіберзахисту, управління доступами та оцінки поточного рівня безпеки у цифровому середовищі.

36. Єдина судова інформаційно-телекомунікаційна система (ЄСІТС).

37. Офіційний веб-портал «Судова влада України».

38. Єдиний державний реєстр судових рішень.

39. Підсистема «Електронний суд».

40. Підсистема «Електронний кабінет».

41. Практичні аспекти подання процесуальних документів в електронній формі, включаючи реєстрацію в системі, створення, підписання та відправлення документів.

42. Оцінка переваг електронного судочинства, таких як оперативність, доступність та зручність роботи.

43. Розгляд викликів і обмежень, пов'язаних із впровадженням електронного судочинства, зокрема технічних, організаційних та правових аспектів.

44. Практичні аспекти подачі документів через систему «Електронний суд» та роботи з електронними доказами.

45. Практика підготовки та подання заяв до ЄСПЛ: основні вимоги, формати документів, електронна комунікація із секретаріатом.

46. Використання Legal Tech для автоматизації рутинних процесів.

47. Інтеграція штучного інтелекту у юридичну діяльність.

48. Використання аналітично-правових систем ZakonOnline, ЛІГА 360, LEXactive для пошуку нормативно-правових актів та судових рішень для розв’язання правових ситуацій та автоматизації рутинних юридичних завдань.

49. Правове обгрунтування фахової діяльності з допомогою Інформаційно-пошукових правових систем.

50. Практичні аспекти роботи з Єдиним державним реєстром судових рішень, базою національного законодавства, актів європейського та міжнародного права.

51. Довідково-інформаційна платформа правових консультацій WikiLegalAid.

52. Мультимедійна підтримка в юридичній діяльності та її практичне значення.

53. Використання технологій для створення мультимедійного контенту.

54. Візуалізація юридичних процесів: інфографіка, ментальні карти (Lucidchart, Miro).

55. Огляд популярних програм і сервісів, таких як Canva, PowerPoint, Prezi, для створення професійного мультимедійного контенту.

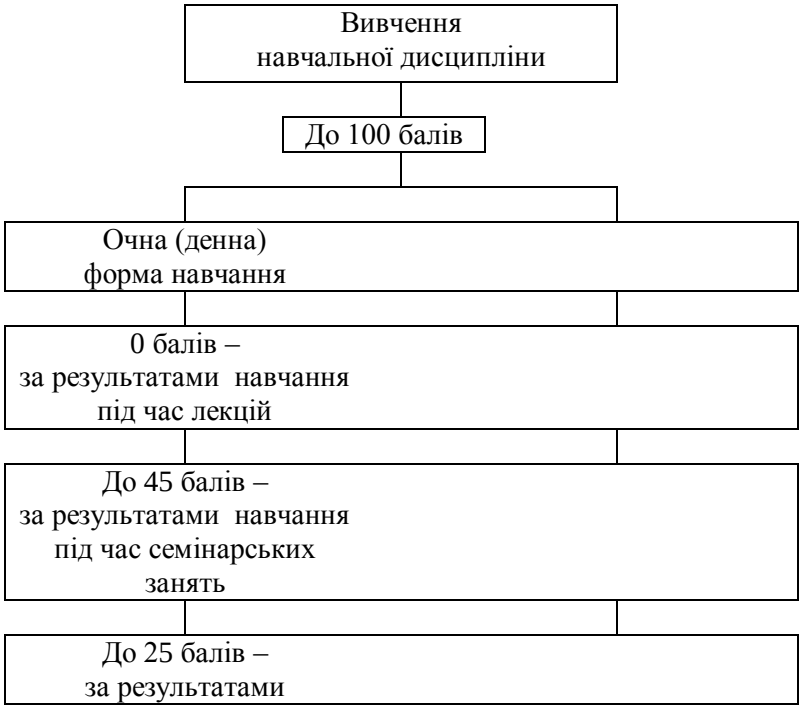
56. Використання відеоконференцзв'язку (Zoom, Google Meet, Microsoft Teams) для організації онлайн-зустрічей із клієнтами та колегами.

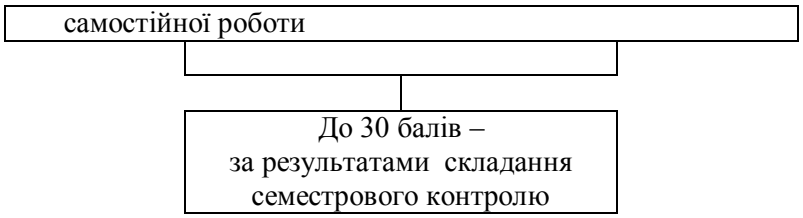
57. Практичні аспекти розміщення мультимедійного контенту на платформах для ефективного донесення інформації.

58. Створення цифрових правничих продуктів для клієнтів, таких як навчальні відео, презентації послуг чи алгоритмів вирішення юридичних питань, відповідно до етичних та правових норм.

2. Схема нарахування балів

2.1. Нарахування балів студентам з навчальної дисципліни здійснюється відповідно до такої схеми:





2.2. Обсяг балів, здобутих студентом під час лекцій з навчальної дисципліни, обчислюється у пропорційному співвідношенні кількості відвіданих лекцій і кількості лекцій, передбачених навчальним планом, і визначається згідно з додатками 1 і 2 до Положення про організацію освітнього процесу в Хмельницькому університеті управління та права імені Леоніда Юзькова.

З цієї навчальної дисципліни лекційний курс не передбачено

2.3. Обсяг балів, здобутих студентом під час семінарських занять, обчислюється за сумою балів, здобутих під час кожного із занять, передбачених навчальним планом, і визначається згідно з додатком 3 до Положення про організацію освітнього процесу в Хмельницькому університеті управління та права.

З цієї навчальної дисципліни передбачено проведення 19 семінарських занять за денною формою навчання.

Отже, рівень знань студентів під час семінарських занять може оцінюватися кількістю балів у таких межах:

№ з/п	Рівень знань студентів		Кількість семінарських занять відповідно до навчального плану
			10 занять
1.	Високий (творчий)	90-100 %	5
2.	Достатній (конструктивно-варіативний)	82-89 %	4,5
		74-81 %	4,0
3.	Середній (репродуктивний)	64-73 %	3,5
		60-63 %	3,0
4.	Низький (рецептивно-продуктивний)	35-59 %	2,0-2,5
		0-34 %	0,5-1,5

2.4. Перерозподіл кількості балів в межах максимально можливої кількості балів за самостійну роботу студентів та виконання індивідуальних завдань, наведено в наступній таблиці:

№ з/п	9 тем	Номер теми									Усього балів
		1	2	3	4	5	6	7	8	9	
1.	Максимальна кількість балів за самостійну роботу	2	2	22	2	2	2	2	2	2	18
2.	Максимальна кількість балів за індивідуальне завдання	7									7
	Усього балів										**25**

3. Рекомендовані джерела

Основні джерела

1. Про інформацію. Закон України від 02.10.1992 р. № 2657–12. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/main/2657-12.
2. Про доступ до публічної інформації. Закон України від 13.01.2011 р. № 2939–VI. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
3. Про Національну програму інформатизації. Закон України від 04.02.1998 р. № 74/98–ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
4. Про науково-технічну інформацію. Закон України від 25.06.1993 р. № 3322–XII. URL: https://zakon.rada.gov.ua/laws/show/3322-12.
5. Про наукову і науково-технічну діяльність. Закон України від 26.11.2015 р. № 848–VIII. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
6. Денисова О. О. Інформаційні системи і технології в юридичній діяльності. Київ : КНЕУ, 2003. 315 с.
7. Козловський А. В., Паночишин Ю. М., Погріщук Б. В. Комп'ютерна техніка та інформаційні технології. 2-е вид. Київ :Знання, 2012. 463 с.
8. Правова інформатика / за ред. В. В. Дурдинця, Є. М. Мойсеева та М. Я. Швеця. Київ : ПанТот, 2007. 524 с.
9. Комп'ютерні технології обробки облікової інформації / за ред. В. Є. Ходакова. Херсон : Олді-плюс; Київ : Ліра-К, 2012. 543 с.
10. Матвієнко М. П., Розен В. П., Закладний О. М. Архітектура комп'ютера. Київ : Ліра-К, 2013. 264 с.
11. Заплотинський Б. А. Інформаційні технології в юридичній діяльності. Київський інститут інтелектуальної власності та права НУ «Одеська юридична академія». Київ, 2018. 108 с.
12. Інформаційні технології / Н. І. Логінова, О. Г. Трофименко, М. А. Яценко, Т. А. Латковська. Одеса, 2024. 152 с. Режим доступу: https://doi.org/10.32837/11300.27258.

Допоміжні джерела

13. Чернега В., Платтнер Б. Безпровідні локальні комп'ютерні мережі. Київ : Кондор, 2013. 238 с.
14. Пічугін М. Ф., Канкін І. О., Воротніков В. В. Комп'ютерна графіка. Київ : ЦУЛ, 2013. 346 с.
15. Інформатика. Комплексні кейси: / за заг. ред. О. Д. Шарапова. Київ : КНЕУ, 2012. 267 с.
16. Буйницька О. П. Інформаційні технології та технічні засоби навчання. Київ : Центр учбової літератури, 2012. 240 с.
17. Басюк Т. М., Думанський Н. О., Пасічник О. В. Основи інформаційних технологій. Львів : Новий Світ – 2000, 2020. 390 с.
18. Кірчук Р. В., Герасимчук О. О., Завіша В. В. Сучасні інформаційні технології. Луцьк : Технічний коледж Луцького НТУ, 2020. 134 с.
19. Інформаційні технології / за ред. О. І. Зачека. Львів : Львівський державний університет внутрішніх справ, 2022. 432 с.
20. Інформаційні технології та моделювання бізнес-процесів / О. М. Томашевський, Г. Г. Цегелик, М. Б. Вітер, В. І. Дудук. Київ : Центр учбової літератури, 2012. 296 с.
21. Інформаційні технології в юридичній діяльності: базовий курс / О. В. Співаковський, М. І. Шерман, В. М. Стратонов, В. В. Лапінський. Херсон : ХДУ, 2012. 220 с.
22. Правова інформація та комп'ютерні технології в юридичній діяльності / за заг. ред. В. Г. Іванова. Харків : Право, 2010. 240 с.

23. Системна інформатизація правоохоронної діяльності / за ред. В. Дурдинця, М. Швеця. Київ : НДЦПІ АПрН України, 2007. 382 с.

8. Інформаційні ресурси в Інтернеті

1. https://www.office.com/
2. Офіційний сайт Верховної Ради України: www.zakon.rada.gov.ua
3. Сайт нормативно-правових документів Кабінету Міністрів України: www.kmu.gov.ua
4. Офіційний сайт Верховного Суду України: www.scourt.gov.ua
5. Офіційний сайт Міністерства Юстиції України: www.gdo.kiev.ua
6. Єдиний портал державних послуг diia.gov.ua
7. Інформаційно-аналітична система Ліга360 igazakon.net
8. Аналітично-правова системаZakonOnline zakononline .com.ua
9. Портал відкритих даних data.gov.ua
10. Портал створення презентацій та інфографіки canva.com
11. Портал створення інфографіки, звітів, презентацій piktochart.com
12. Портал судової влади в Україні court.gov.ua
13. Хмарний сервіс Google Диск
14. Prometheus. Електронний ресурс: https://prometheus.org.ua/
15. Microsoft Imagine Academy. Електронний ресурс: https://imagineacademy.microsoft.com/?whr=default
16. Cisco Networking Academy. Електронний ресурс: https://www.netacad.com/
17. Топ-10 корисних мобільних додатків для юристів, LOЙEP [Електронний ресурс]. Режим доступу: http://loyer.com.ua/uk/top-10-korisnihmobilnih-dodatkiv-dlya-yuristiv/
18. Планета Excel: коли знаєш все просто [Електронний ресурс]. Режим доступу: http://www.planetaexcel.ru/
19. Навчальний сайт «Інформаційні системи та технології»: http://informatic-10.at.ua/index/informacijni sistemi ta tekhnologiji/0-29/