Практичне заняття № 2

Тема: Правове регулювання доступу до інформації. Захист інформації з обмеженим доступом.

Мета: Ознайомити студентів із правовим регулюванням доступу до інформації та захисту інформації з обмеженим доступом, навчити аналізувати офіційні веб-сайти органів влади, розрізняти види інформації та оцінювати правомірність обмежень доступу.

Питання для обговорення:

1. Основи правового регулювання доступу до публічної інформації в Україні.

2. Принципи прозорості та відкритості державних електронних інформаційних ресурсів: як забезпечується доступ громадян до даних.

3. Офіційні веб-сайти органів державної влади та місцевого самоврядування: механізми доступу, стандарти вебдоступності, цифрові сервіси.

4. Види інформації з обмеженим доступом.

5. Особливості правового режиму державної таємниці: порядок засекречування, класифікація ступенів секретності, строки дії рішень, правові наслідки порушень.

6. Практичні проблеми реалізації права на інформацію: обмеження доступу, конфлікт між публічністю та захистом державних інтересів.

7. Використання принципу пропорційності при обмеженні доступу до інформації: критерії оцінки законності та обґрунтованості обмежень.

8. Цифрові виклики та загрози інформаційній безпеці: кіберзлочини, несанкціонований доступ до державних електронних ресурсів, витоки даних.

9. Кейси з порушення доступу до публічної інформації та розголошення державної таємниці: аналіз реальних ситуацій і правові наслідки.

10. Перспективи розвитку законодавства про доступ до інформації та захист інформації з обмеженим доступом: роль міжнародних стандартів і цифровізації.

✍Практичні завдання:

1. Проаналізуйте офіційний веб-сайт органу державної влади або органу місцевого самоврядування (за вибором). Визначте, які розділи веб-сайту містять публічну інформацію. З'ясуйте, чи передбачено механізм подання запиту на публічну інформацію. Оцініть повноту та доступність оприлюдненої інформації.

Форма виконання: аналітична таблиця з такими графами: назва розділу веб-сайту - вид інформації - нормативне обґрунтування - висновок щодо доступності.

2. Керівник структурного підрозділу органу виконавчої влади присвоїв документу гриф «таємно», мотивуючи це тим, що документ містить внутрішню аналітичну інформацію щодо підготовки управлінського рішення. Визначте, чи може така інформація бути віднесена до державної таємниці. Відмежуйте державну таємницю від службової інформації. Оцініть правомірність дій посадової особи. *Форма виконання: письмовий правовий висновок (до 1 сторінки).*

3. Внутрішній ІТ-документ органу влади з описом архітектури кіберзахисту був позначений як службова інформація. Після кібератаки громадська організація вимагає його оприлюднення, посилаючись на суспільний інтерес. Відмежуйте службову інформацію від таємної. *Оцініть пропорційність обмеження доступу.*

4. Орган виконавчої влади відмовив у доступі до екологічного звіту, посилаючись на те, що документ містить відомості про об'єкти критичної інфраструктури і має гриф «таємно». Згодом з'ясувалося, що рішення про засекречування приймалося не державним експертом з питань таємниць. Оцініть юридичну чинність рішення про засекречування. Визначте правові наслідки для органу влади. Обґрунтуйте алгоритм відновлення доступу до інформації. *Форма виконання: письмовий правовий висновок із блок-схемою процедури*.

5. Журналіст онлайн-видання звернувся із запитом на публічну інформацію до державного органу щодо структури витрат бюджетних коштів на забезпечення функціонування захищених інформаційно-телекомунікаційних систем органу влади за попередній рік. У відповіді на запит орган влади відмовив у наданні інформації, зазначивши, що: запитувані відомості містяться у внутрішніх аналітичних звітах, які мають гриф «Для службового користування»; оприлюднення структури витрат може дозволити встановити архітектуру та вразливості інформаційних систем; частина відповідної інформації використовується у документах, віднесених до державної таємниці у сфері державної безпеки. Водночас на офіційному вебсайті органу влади у розділі «Використання бюджетних коштів» оприлюднені загальні суми фінансування без деталізації, а рішення державного експерта з питань таємниць щодо віднесення запитуваної інформації до державної таємниці не оприлюднювалося і

до відповіді на запит додано не було. Журналіст оскаржує відмову, посилаючись на принцип відкритості бюджетної інформації, суспільний інтерес та право на доступ до інформації. *Визначте правову природу запитуваної інформації та віднесіть її до відповідного виду інформації. Проаналізуйте правомірність застосування грифу «Для службового користування» у наведеній ситуації. Оцініть, чи може інформація про використання бюджетних коштів бути віднесена до державної таємниці. Визначте правові механізми захисту права журналіста на доступ до інформації.*

Методичні рекомендації до виконання практичного заняття

Опрацювання теоретичних питань:

Під час підготовки відповідей рекомендується поєднувати правові, соціальні та цифрові підходи до розуміння інформації. Особливу увагу приділити розмежуванню понять «публічна інформація», «службова інформація» та «державна таємниця», спираючись на відповідні закони України. При аналізі інформаційних відносин визначати суб'єктний склад, об'єкт та зміст прав і обов'язків, наводячи приклади з діяльності державних органів, органів місцевого самоврядування або цифрових сервісів.

Виконання практичних завдань (таблична форма, письмові висновки, блок-схеми): Аналіз нормативних актів проводити за логікою: норма → правова категорія → практичний приклад. При заповненні таблиць використовувати приклади реальних або наближених до практики ситуацій (офіційні веб-сайти, електронні сервіси, документи з грифами «таємно» або «для службового користування»). Відображати особливості доступу до інформації та правомірність обмежень з урахуванням принципу пропорційності.

Аналіз загроз інформаційній безпеці:

Обираючи загрозу (кібератаки, несанкціонований доступ, витік даних), поєднувати технічний аспект з правовим аналізом. Чітко зазначати, які норми законодавства (інформаційного, адміністративного, кримінального) застосовуються для захисту від конкретної загрози.