

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту Закону України про внесення змін до статті 190
Кримінального кодексу України щодо криміналізації протиправних
(шахрайських) діянь, вчинених із використанням інформаційно-
комунікаційних систем або систем штучного інтелекту

1. Обґрунтування необхідності прийняття проєкту Закону

Необхідність прийняття цього законопроєкту зумовлена стрімким розвитком цифрових технологій, що призвело до появи принципово нових високотехнологічних способів учинення злочинів проти власності.

Масштабність даної проблеми та динаміка зростання злочинів, що вчиняються із застосуванням сучасних інформаційно-комунікаційних систем та штучного інтелекту підтверджується офіційними статистичними даними Офісу Генерального прокурора та Національного банку України:

- за даними Офісу Генерального прокурора, рівень шахрайства в Україні залишається критично високим. Після історичного піка у 2023 році (82 609 кримінальних справ) та майже 65 000 проваджень у 2024 році, за підсумками 2025 року було зафіксовано 48 871 справу за статтею 190 ККУ. Попри певне зниження загальної кількості зареєстрованих кримінальних проваджень в порівнянні з піковими періодами війни, цей показник усе ще вдвічі перевищує рівень до повномасштабного вторгнення (у 2021 році було зареєстровано 23 847 справ);

- згідно зі статистикою Національного банку України, 83% від загальної кількості всіх шахрайських операцій із платіжними картками здійснюються саме в мережі Інтернет (із використанням інформаційно-комунікаційних систем та методів соціальної інженерії). За даними офіційних досліджень цифрової та ІТ-грамотності, станом на кінець 2025 року - початок 2026 року, близько 23% українців особисто стикалися з кібератаками та шахрайськими схемами, посиленими штучним інтелектом, а 35% дорослого населення отримували згенеровані штучним інтелектом фейкові відповіді чи контент;

- попри превентивні заходи та незначне зменшення кількості незаконних транзакцій (із 270 тис. операцій у 2024 році до 256 тис. у 2025 році), масштаби фінансових втрат громадян стрімко зростають. За підсумками 2025 року загальна сума збитків від шахрайства з використанням платіжних карток збільшилася на 24% та сягнула 1,4 мільярда гривень. Це пов'язано з підвищенням технологічної складності атак та зростанням обсягу середньої суми однієї злочинної операції на 30% - з 4 247 грн до 5 536 грн.

Традиційні механізми захисту, закріплені у статті 190 Кримінального кодексу України, наразі не повною мірою враховують специфіку та суспільну небезпеку правопорушень, які вчиняються в цифровому просторі.

Окремим критичним аспектом чинного кримінального законодавства є використання застарілої термінології. Діюча редакція диспозиції статті 190 Кримінального кодексу України оперує поняттям «електронно-обчислювальна техніка», яке є термінологічним анахронізмом, сформованим

ще наприкінці ХХ століття. У сучасних умовах тотальної цифровізації, хмарних обчислень та мережевої інтеграції використання цього терміну є юридично некоректним та таким, що створює штучні прогалини у правозастосуванні. Злочинні посягання сьогодні здійснюються не просто на окремих фізичних пристроях (ЕОМ), а в межах складних, розподілених мереж, платформ та систем.

У зв'язку з викладеним вище, виникла нагальна потреба модернізувати кримінальне законодавство та замінити архаїчний термін «електронно-обчислювальна техніка» на уніфіковане та технологічно нейтральне поняття «інформаційно-комунікаційні системи» (ІКС), яке повністю відповідає сучасному профільному базовому законодавству України (зокрема Закону України «Про захист інформації в інформаційно-комунікаційних системах»).

Паралельно з цим, правова база потребує негайного реагування на появу систем штучного інтелекту (ШІ). Зловмисники дедалі частіше використовують технології синтезу мовлення, генерації текстового контенту та створення візуальних «дипфейків» для введення громадян в оману. Штучний інтелект дозволяє масово автоматизувати процеси психологічного маніпулювання, імітувати голоси чи обличчя близьких родичів постраждалих, створювати фіктивні інвестиційні та брокерські платформи із реалістичними котируваннями, що призводить до катастрофічних матеріальних збитків для населення. Відсутність чіткої кваліфікації таких діянь як окремої кваліфікуючої ознаки злочину ускладнює досудове розслідування та формування належної судової практики.

2. Цілі та завдання проєкту Закону

Основною метою законопроєкту є посилення кримінальної відповідальності за шахрайство, вчинене за допомогою інформаційно-комунікаційних систем або систем штучного інтелекту, а також законодавче закріплення понятійно-термінологічного апарату для ідентифікації таких правопорушень.

Завданнями акта є: мінімізація рівня кіберзлочинності та шахрайських схем у цифровому просторі; удосконалення правових інструментів захисту майнових прав громадян від маніпулятивних технологій нового покоління та створення правових підстав для залучення експертів із кібербезпеки до верифікації ШІ-генерацій у межах кримінальних проваджень.

3. Загальна характеристика і основні положення проєкту Закону

Проєкт Закону передбачає комплексну модернізацію статті 190 Кримінального кодексу України шляхом оновлення понятійного апарату відповідно до вимог часу, зокрема:

1) абзац перший частини четвертої статті викладається в новій редакції, яка відносить до кваліфікованих складів злочину шахрайство, вчинене шляхом незаконних операцій із використанням інформаційно-комунікаційних систем або систем штучного інтелекту;

2) стаття доповнюється приміткою, положеннями якої:

- термін «інформаційно-комунікаційні системи» застосовується/вживається у цій статті у значенні, визначеному в Законі України «Про захист інформації в інформаційно-комунікаційних системах» (*частина перша примітки*);

- у кримінальному праві закріплюється поняття «системи штучного інтелекту», під якими розуміються технологічні системи (програмне забезпечення або програмно-апаратні комплекси), які здатні генерувати контент, прогнози, рекомендації чи рішення, що мають ознаки інтелектуальної діяльності людини та використовуються для введення потерпілого в оману (зокрема за допомогою технологій заміни чи модифікації обличчя, голосу або текстових даних - технологій дипфейків) (*частина друга примітки*).

3) у Прикінцевих положеннях до законопроекту, Кабінету Міністрів України доручається у місячний строк забезпечити прийняття необхідних підзаконних актів. Зокрема, передбачено створення чіткого процесуального механізму із залученням експертів з кібербезпеки для верифікації ШІ-генерацій під час досудового розслідування та судового розгляду кримінальних проваджень.

4. Стан нормативно-правової бази у даній сфері правового регулювання

Регулювання у цій сфері здійснюється Конституцією України, Кримінальним кодексом України, Законом України «Про захист інформації в інформаційно-комунікаційних системах», іншими нормативно-правовими актами.

Реалізація положень законопроекту не потребує внесення змін до інших законів України.

5. Фінансово-економічне обґрунтування проєкту Закону

Реалізація даного законопроекту не потребує додаткових витрат з Державного бюджету України.

6. Прогноз соціально-економічних та інших наслідків прийняття проєкту Закону

Прийняття Закону дозволить правоохоронним органам ефективно протидіяти технологічному шахрайству, забезпечить невідворотність покарання за кіберзлочини з використанням штучного інтелекту, підвищить загальний рівень захищеності майнових прав і цифрової безпеки громадян України та наблизить вітчизняне кримінальне законодавство до європейських та світових стандартів у сфері регулювання штучного інтелекту та протидії кіберзлочинності. (зокрема, у контексті адаптації до положень Регламенту ЄС про штучний інтелект (AI Act)).

Народні депутати України

С.В. Кузьмініх та інші

