

ПОЛОЖЕННЯ

про використання систем штучного інтелекту працівниками Апарату Верховного Суду

Розділ I. Загальні положення

1. Предмет і сфера дії Положення

1.1. Це Положення визначає правила використання систем штучного інтелекту працівниками Апарату Верховного Суду під час виконання службових обов'язків.

1.2. Положення поширюється на державних службовців, працівників патронатної служби та інших працівників Апарату Верховного Суду, які використовують, впроваджують, адмініструють, супроводжують або оцінюють системи штучного інтелекту.

1.3. Положення застосовується до загальнодоступних, корпоративних, локальних, хмарних і вбудованих систем штучного інтелекту, а також до систем, наданих Верховному Суду в межах міжнародної технічної допомоги, дослідних проєктів або інших форм співпраці.

1.4. Положення не регулює зміст процесуальної діяльності суддів під час здійснення правосуддя та не може тлумачитися як дозвіл на заміну, обмеження чи автоматизоване формування суддівського розсуду.

1.5. У частині використання систем штучного інтелекту працівниками патронатної служби під час підготовки справ до розгляду це Положення застосовується з урахуванням того, що такі працівники з цих питань підзвітні відповідному судді.

2. Нормативна основа

2.1. Положення застосовується відповідно до Конституції України, законів України «Про судоустрій і статус суддів», «Про державну службу», «Про інформацію», «Про доступ до публічної інформації», «Про доступ до судових рішень», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про авторське право і суміжні права», «Про санкції», процесуального законодавства України, міжнародних договорів України, статті 16 Кодексу суддівської етики, затвердженого рішенням XX з'їзду суддів України від 18 вересня 2024 року, Положення про Апарат Верховного Суду, затвердженого постановою Пленуму Верховного Суду від 30 листопада 2017 року № 6, та інших актів Верховного Суду.

2.2. Під час застосування цього Положення можуть враховуватися як орієнтири для його тлумачення та застосування, якщо вони не суперечать законодавству України:

2.2.1. Європейська етична хартія щодо використання штучного інтелекту в судових системах та їхньому середовищі, ухвалена Європейською комісією з питань ефективності правосуддя (СЕРЕJ) у грудні 2018 року;

2.2.2. Висновок № 26 (2023) Консультативної ради європейських суддів «Рухаючись вперед: використання допоміжних технологій у судочинстві»;

2.2.3. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту;

2.2.4. методологія Ради Європи щодо оцінювання ризиків і впливу систем штучного інтелекту на права людини, демократію та верховенство права (HUDERIA);

2.2.5. Поради з відповідального використання штучного інтелекту публічними службовцями, розроблені Міністерством цифрової трансформації України спільно з партнерами у 2025 році;

2.2.6. Рекомендації для правників щодо відповідального використання штучного інтелекту, підготовлені Міністерством юстиції України спільно з національними та міжнародними партнерами у 2025 році;

2.2.7. Словник термінів у сфері штучного інтелекту, розроблений Міністерством цифрової трансформації України спільно з Експертно-консультаційним комітетом з питань розвитку сфери штучного інтелекту в Україні, 2024 рік;

2.2.8. Коментар до Кодексу суддівської етики, затверджений рішенням Ради суддів України від 02 березня 2026 року № 14, — у частині, що стосується статті 16 Кодексу суддівської етики.

3. Основні терміни

3.1. У цьому Положенні терміни вживаються у такому значенні:

3.1.1. система штучного інтелекту (система ШІ) — машинна система, яка з певним рівнем автономності та для явно або неявно визначених цілей на підставі отриманих вхідних даних формує результати, зокрема прогнози, рекомендації, тексти, зображення чи класифікації, що можуть впливати на фізичне чи цифрове середовище;

3.1.2. загальнодоступна система ШІ — система, доступна невизначеному колу користувачів і щодо якої Верховний Суд не має договору або іншого правового механізму, що визначає умови обробки та захисту службових даних;

3.1.3. корпоративна система ШІ — система, доступ до якої надано Верховному Суду на договірних, ліцензійних або інших визначених правових засадах із установленими умовами захисту даних, доступу та відповідальності постачальника;

3.1.4. локальна система ШІ — система, що працює у захищеному інформаційному середовищі Верховного Суду без передання даних зовнішньому постачальнику;

3.1.5. схвалений спосіб використання — визначене поєднання системи ШІ, службової мети, категорій даних, кола користувачів, технічного середовища та встановлених обмежень, дозволене для застосування в Апараті Верховного Суду;

3.1.6. захищені дані — інформація з обмеженим доступом, а також інші відомості, щодо яких законодавством або цим Положенням встановлено спеціальні обмеження використання, зокрема неопублічні матеріали судових справ, внутрішні проекти документів, службове листування, записи службових нарад та персональні дані, що не є правомірно оприлюдненими;

3.1.7. профілювання — автоматизована обробка даних про особу з метою оцінювання або прогнозування її особистих, професійних, поведінкових чи інших характеристик;

3.1.8. істотне використання системи ШІ — використання, яке вплинуло на змістовні висновки, аргументацію, добір джерел, оцінку інформації або інший змістовний елемент службового документа чи аналітичного матеріалу;

3.1.9. інцидент – подія, пов'язана з використанням системи ШІ, яка призвела або могла призвести до розголошення захищених даних, неправомірної обробки персональних даних, використання недостовірного результату, несанкціонованого доступу, порушення вимог цього Положення або іншої істотної шкоди;

3.1.10. уповноважений структурний підрозділ – структурний підрозділ або кілька підрозділів Апарату Верховного Суду, визначені керівником Апарату для ведення Реєстру, методичного супроводу, оцінювання ризиків, моніторингу, навчання та реагування на інциденти;

3.1.11. зовнішня система ШІ – система ШІ, що використовує технічну інфраструктуру, програмне середовище або послуги зовнішнього постачальника для обробки запитів, даних чи результатів;

3.1.12. вбудована офісна функція ШІ – функція ШІ, інтегрована до програмного забезпечення, яке використовується Верховним Судом для підготовки, редагування, пошуку, перекладу, перетворення мовлення на текст або іншої технічної обробки документів.

3.2. Перевірка правопису, форматування, технічне структурування, автоматичне перетворення мовлення на текст і попередній переклад без зміни змісту самі по собі не є істотним використанням системи ШІ.

4. Основні принципи

4.1. Використання систем ШІ ґрунтується на таких принципах:

4.1.1. верховенство права, законність і повага до прав людини;

4.1.2. незалежність суддів і невтручання у здійснення правосуддя;

4.1.3. допоміжний характер систем ШІ та обов'язковий людський контроль;

4.1.4. особиста відповідальність працівника за результат його роботи;

4.1.5. достовірність, перевірність і використання першоджерел;

4.1.6. захист інформації, кібербезпека та мінімізація даних;

4.1.7. недискримінація та недопущення необґрунтованого профілювання;

4.1.8. відповідність заходів контролю рівню ризику конкретного способу використання;

4.1.9. прозорість та можливість внутрішньої перевірки істотного використання систем ШІ.

Розділ II. Допустиме використання та заборони

5. Загальні умови допустимого використання

5.1. Працівник може використовувати систему ШІ лише для службового завдання, що належить до його повноважень, за умови дотримання цього Положення та встановлених для відповідного способу використання обмежень.

5.2. Система ШІ використовується як допоміжний засіб. Працівник самостійно формує зміст документа, висновку або рекомендації, які він готує. Управлінське рішення приймає уповноважена посадова особа, яка не може покладатися виключно на результат роботи системи ШІ.

5.3. У разі сумніву щодо допустимості системи, категорії даних або способу використання працівник утримується від такого використання до отримання роз'яснення уповноваженого структурного підрозділу або рішення про схвалення відповідного способу використання.

5.4. Сумніви щодо допустимості використання системи ШІ тлумачаться на користь захисту незалежності суду, прав людини, інформаційної безпеки та конфіденційності.

5.5. Добросовісна відмова працівника від використання системи ШІ через обґрунтовані сумніви щодо безпеки, законності або достовірності результату не може сама по собі бути підставою для негативної оцінки його роботи, якщо про такі сумніви своєчасно повідомлено безпосереднього керівника або уповноважений структурний підрозділ.

6. Незалежність суддів і межі використання у судовій діяльності

6.1. Системи ШІ не можуть використовуватися для підміни, нав'язування або автоматизованого формування суддівського розсуду, внутрішнього переконання судді, оцінки доказів, встановлення фактичних обставин, правової кваліфікації, правової позиції або результату розгляду конкретної справи.

6.2. Забороняється використовувати системи ШІ для:

6.2.1. автоматизованого прогнозування рішення судді, складу суду або результату розгляду конкретної справи;

6.2.2. моделювання позиції конкретного судді або складу суду в конкретній справі;

6.2.3. автоматизованого індивідуального рейтингового, поведінкового або прогностичного оцінювання судді за змістом рішень, стилем письма, категоріями справ, складом колегій або іншими параметрами;

6.2.4. прихованого спостереження, розпізнавання емоцій, біометричної категоризації, психологічного чи поведінкового профілювання суддів;

6.2.5. одержання, використання або розголошення інформації, що відповідно до процесуального закону становить таємницю ухвалення судового рішення;

6.2.6. створення засобів впливу, тиску або маніпуляції щодо суддів;

6.2.7. втручання в автоматизований розподіл судових справ або роботу автоматизованої системи документообігу суду;

6.2.8. автоматичного створення проєктів постанов, ухвал, окремих думок суддів або інших процесуальних актів;

6.2.9. обходу встановлених правил документообігу, кібербезпеки, контролю доступу, погодження документів або інших обов'язкових внутрішніх процедур.

6.3. Аналітичне опрацювання відкритої судової практики допускається для узагальнення практики, виявлення системних правових проблем, підготовки статистичних, наукових та аналітичних матеріалів, якщо воно не використовується для індивідуального оцінювання або прогнозування поведінки суддів.

6.4. Система ШІ не може застосовуватися у спосіб, який приховано вилучає, вибірково відображає, ранжує або спотворює доводи, докази чи правові позиції, що можуть мати значення для змагальності, рівності сторін і права на справедливий суд.

7. Використання систем ШІ працівниками патронатної служби

7.1. Працівник патронатної служби з питань підготовки справ до розгляду використовує систему ШІ лише за дорученням відповідного судді та в межах такого доручення. Доручення може стосуватися конкретної справи або визначених видів допоміжних завдань у справах відповідної

категорії; воно не може розширювати дозволені цим Положенням способи використання систем ШІ.

7.2. Для пошуку, добору, узагальнення та впорядкування відкритих джерел працівник патронатної служби може використовувати системи ШІ на тих самих умовах, що й інші працівники Апарату.

7.3. Опрацювання непублічних матеріалів судової справи допускається лише у схваленій системі в захищеному середовищі та лише для способу використання, внесеного до Реєстру.

7.4. У межах пункту 7.3 допускаються:

7.4.1. структурування матеріалів справи;

7.4.2. підготовка стислого викладу доводів і заперечень учасників справи без їх оцінювання;

7.4.3. складання таблиць, переліків та інших допоміжних матеріалів;

7.4.4. перевірка реквізитів, посилань і цитат за офіційними або іншими надійними першоджерелами;

7.4.5. технічна підготовка описових або довідкових частин аналітичних довідок, оглядів, таблиць та інших допоміжних матеріалів без формування правового висновку за суддю.

7.5. Стислий виклад доводів і заперечень обов'язково звіряється з оригінальними матеріалами справи на точність і повноту. Істотний довід або заперечення не може бути виключений лише внаслідок автоматизованого відбору чи скорочення.

7.6. Система ШІ не може самостійно визначати, які факти вважати встановленими, оцінювати докази, вирішувати питання їх допустимості чи достатності, формувати правовий висновок у конкретній справі або створювати текст мотивувальної чи резолютивної частини судового рішення.

7.7. Проект судового рішення, що не оприлюднений, для цілей цього Положення підлягає режиму захищених даних. Його обробка у загальнодоступній системі ШІ забороняється. У корпоративній, хмарній чи іншій зовнішній системі така обробка допускається лише після схвалення відповідного способу використання та середовища для цієї категорії даних. Обробка такого проекту в корпоративній, хмарній чи іншій зовнішній системі може бути схвалена лише за умови дотримання вимог пункту 15.4 цього Положення. Вбудовані офісні функції, що відповідають умовам пункту 10.2 цього Положення, можуть застосовуватися до проекту судового рішення без окремого схвалення для суто технічної перевірки правопису, форматування та друкарських помилок без зміни змісту. Якщо проект або пов'язані з ним матеріали містять відомості, що відповідно до процесуального закону становлять таємницю ухвалення судового рішення, такі відомості не можуть оброблятися системою ШІ.

7.8. Істотне використання системи ШІ під час підготовки для судді аналітичної довідки, огляду практики, добірки джерел або іншого матеріалу фіксується, а суддя інформується про факт такого використання у порядку, затвердженому керівником Апарату Верховного Суду. Таке інформування не переносить на суддю відповідальність працівника за точність і повноту підготовленого матеріалу.

7.9. Відомості із закритого судового засідання можуть оброблятися із використанням системи ШІ лише в локальній системі ШІ, для способу використання, окремо схваленого для цієї категорії даних відповідно до пункту 20.3 цього Положення, та за дорученням судді, у провадженні якого перебуває справа. Обробка таких відомостей у корпоративній, хмарній або іншій зовнішній системі ШІ забороняється.

8. Дозволені напрями використання

8.1. За умови дотримання цього Положення системи ШІ можуть використовуватися для:

8.1.1. пошуку, узагальнення, класифікації та тематичного впорядкування відкритої судової практики, законодавства, міжнародних документів, наукових та інших відкритих джерел;

8.1.2. підготовки попередніх аналітичних, інформаційних, навчальних і звітних матеріалів;

8.1.3. наповнення та технічного впорядкування Базы правових позицій Верховного Суду за умови перевірки працівником кожного змістовного елемента до його внесення;

8.1.4. технічного редагування, скорочення, структурування та уніфікації термінології без зміни правового змісту;

8.1.5. попереднього перекладу з обов'язковою фаховою перевіркою;

8.1.6. сортування відкритих даних, підготовки таблиць, графіків, діаграм, шаблонів та інших технічних матеріалів;

8.1.7. підготовки проєктів інформаційних і комунікаційних матеріалів, що не містять захищених даних і не відображають позицію Верховного Суду щодо суті конкретної справи;

8.1.8. підготовки проєктів відповідей на звернення та запити: з відкритою інформацією — у системах, дозволених для відповідного рівня ризику; із захищеними даними — лише у схваленій захищеній системі;

8.1.9. автоматизованого виявлення відомостей, що підлягають знеособленню у текстах судових рішень перед оприлюдненням, лише у схваленій захищеній системі та за умови обов'язкової перевірки працівником;

8.1.10. створення автоматизованих довідкових сервісів із питань загального характеру;

8.1.11. інших допоміжних завдань, якщо вони не заборонені цим Положенням і відповідають умовам схваленого способу використання.

8.2. Текст, підготовлений або відредагований із використанням системи ШІ, має відповідати нормам української літературної мови, офіційно-діловому стилю, вимогам юридичної точності, термінологічної послідовності, зрозумілості та лаконічності, а також установленим у Верховному Суді правилам оформлення документів.

8.3. Використання систем ШІ не повинно призводити до плагіату, прихованого запозичення, порушення авторського права чи інших прав інтелектуальної власності, а також до невинуватеного передання постачальнику системи прав на службові матеріали.

9. Управлінські рішення та захист працівників

9.1. Кадрове, дисциплінарне, фінансове або інше управлінське рішення, що стосується прав, обов'язків чи законних інтересів особи, не може прийматися виключно на підставі рекомендації, оцінки, рейтингу або іншого результату системи ШІ.

9.2. Працівникові має бути забезпечена можливість людського перегляду автоматизованої рекомендації, якщо така рекомендація використовується під час підготовки управлінського рішення щодо нього.

9.3. Забороняється використовувати системи ШІ для прихованого спостереження, розпізнавання емоцій, біометричної категоризації, психологічного чи поведінкового профілювання працівників, а також для створення автоматизованих рейтингів працівників без прямої правової підстави.

10. Загальнодоступні та вбудовані системи

10.1. Без окремого схвалення загальнодоступні системи ШІ можуть використовуватися для способів низького ризику з відкритою інформацією, визначених пунктом 1 Додатка 2 та Додатком 1. Аналітичне узагальнення відкритої судової практики або інше істотне використання загальнодоступної системи потребує попереднього схвалення відповідного способу використання та внесення його до Реєстру.

10.2. Вбудовані офісні функції ШІ можуть використовуватися без окремого схвалення з внутрішніми службовими документами, якщо одночасно:

10.2.1. функція не створює самостійного юридично значущого змісту;

10.2.2. дані не передаються за межі захищеного інформаційного середовища Верховного Суду або іншого середовища, окремо дозволеного для таких даних;

10.2.3. функція не використовується для аналізу поведінки, продуктивності або професійних якостей працівників чи суддів;

10.2.4. її використання не впливає на права, обов'язки чи правове становище осіб.

10.3. До функцій, зазначених у пункті 10.2, можуть належати перевірка правопису, автодоповнення окремих слів, технічне форматування, пошук друкарських помилок та інші суто технічні операції без зміни змісту документа.

11. Особисті облікові записи, автоматичне перетворення мовлення на текст та автономні засоби

11.1. Для службових завдань забороняється використовувати особисті облікові записи у системах ШІ, якщо до системи передаються захищені дані або службові матеріали, а також установлювати несхвалені програмні розширення чи засоби, що мають доступ до службової пошти, документів, календарів або інформаційних систем Верховного Суду.

11.2. Автоматичне перетворення мовлення на текст під час службових нарад, консультацій, відеоконференцій або інших внутрішніх обговорень допускається лише у схваленій системі, за наявності службової потреби та з дотриманням правил доступу і зберігання відповідного запису.

11.3. Системи ШІ, здатні самостійно виконувати дії від імені користувача, зокрема надсилати повідомлення, змінювати файли, здійснювати пошук у внутрішніх сховищах або взаємодіяти з іншими інформаційними системами, можуть використовуватися лише після окремого схвалення та визначення меж їх повноважень, контролю доступу і способу припинення дій.

12. Зовнішня комунікація та штучно створені матеріали

12.1. Матеріал, підготовлений із використанням системи ШІ для зовнішнього оприлюднення, підлягає змістовній, правовій та мовній перевірці відповідальним працівником і не може вводити в оману щодо авторства, джерела, обставин або офіційної позиції Верховного Суду.

12.2. Аудіо-, відео- чи фотоматеріали, згенеровані з використанням систем ШІ, що імітують конкретного суддю або працівника Верховного Суду та можуть бути сприйняті як справжні, можуть виготовлятися або поширюватися лише за попередньою згодою такої особи та за умови належного маркування.

12.3. Забороняється створювати матеріали, що імітують офіційне повідомлення або позицію Верховного Суду та можуть бути сприйняті як справжні.

13. Автоматизовані довідкові сервіси

13.1. Автоматизовані довідкові сервіси можуть надавати загальну інформацію про діяльність Верховного Суду, порядок звернення, навігацію офіційними електронними ресурсами та іншу довідкову інформацію.

13.2. Такі сервіси не можуть надавати правову консультацію щодо конкретної справи, прогнозувати результат її розгляду, створювати враження спілкування із суддею або уповноваженим працівником чи подавати свою відповідь як офіційну позицію суду.

13.3. Користувач до початку взаємодії має бути чітко поінформований, що взаємодіє з автоматизованим сервісом і що його відповіді мають довідковий характер.

13.4. Користувачеві забезпечується зрозуміла можливість звернутися до уповноваженого працівника Верховного Суду з питання, яке виходить за межі довідкової функції сервісу.

14. Перевірка результатів і фіксація істотного використання

14.1. Результат роботи системи ШІ не має самостійної доказової, нормативної або офіційної сили та не є першоджерелом.

14.2. До використання у службовій діяльності працівник перевіряє фактичні дані, джерела, цитати, реквізити, дати, переклад і правові висновки за офіційними або іншими надійними першоджерелами. Для нормативно-правового акта перевіряється чинність і редакція, що підлягає застосуванню; для судового рішення — його актуальність, а за потреби також наявність відступу від відповідної правової позиції або її зміни.

14.3. Якщо результат містить стислий виклад документа, доводів або значного масиву інформації, працівник перевіряє не лише точність, а й повноту відображення істотних положень.

14.4. Непереверена інформація не може подаватися як достовірна. Якщо перевірити джерело або твердження неможливо, воно не використовується як підтверджене.

14.5. Істотне використання системи ШІ у матеріалі, що передається судді, або в документі, призначеному для зовнішнього адресата, фіксується у порядку, затвердженому керівником Апарату Верховного Суду.

14.6. Про істотне використання системи ШІ у документі, що надсилається зовнішньому адресату або оприлюднюється, зазначається в самому документі або в супровідній інформації, якщо інше не встановлено законом. Таке зазначення не вимагається, якщо система ШІ використовувалася лише для операцій, визначених пунктом 3.2 цього Положення.

14.7. Фіксація та інформування адресата не звільняють працівника від обов'язку перевірки та не переносять на адресата відповідальність за зміст підготовленого матеріалу.

14.8. Попередній переклад, виконаний системою ШІ, підлягає фаховій перевірці. Він не замінює фахового перекладу у випадках, коли такий переклад потрібний за законом або характером документа, і не може подаватися як остаточний офіційний текст без перевірки уповноваженою особою.

14.9. Якщо під час дозволеного опрацювання матеріалів справи працівник виявив у документі учасника справи посилання на неіснуюче судове рішення, нормативно-правовий акт, інше

джерело або істотно спотворену цитату, він перевіряє відповідні відомості, фіксує виявлену невідповідність та повідомляє про неї суддю, не роблячи припущень щодо причин її виникнення.

Розділ III. Дані, зовнішні системи та кібербезпека

15. Обробка даних та умови використання зовнішніх систем

15.1. Обробка захищених даних із використанням системи ШІ допускається лише за наявності правової підстави, службової необхідності та схваленого способу використання у захищеному середовищі, крім випадків, прямо передбачених пунктами 7.7 і 10.2 цього Положення.

15.2. У загальнодоступні системи ШІ забороняється вводити непублічні матеріали судових справ, внутрішні проекти документів, службове листування, записи внутрішніх нарад, відомості із закритих судових засідань, інформацію з обмеженим доступом та інші захищені дані.

15.3. Відкриті персональні дані або номери оприлюднених судових справ можуть використовуватися лише за наявності службової мети та в обсязі, необхідному для відповідного завдання. Дані, які у сукупності розкривають непублічний контекст конкретної справи або особи, до загальнодоступних систем не вводяться.

15.4. У разі обробки захищених даних у зовнішній системі ШІ умови її використання мають виключати використання введених даних, запитів і результатів для навчання або вдосконалення моделей постачальника чи третіх осіб. Строки зберігання таких даних мають бути мінімізовані, доступ постачальника і третіх осіб — обмежений технічно й організаційно, а порядок доступу, журналювання та видалення даних — визначений до початку використання системи. Під час роботи з відкритою інформацією налаштування, що забороняють використання введених даних, запитів і результатів для навчання або вдосконалення моделей, застосовуються, якщо вони технічно доступні.

15.5. Не допускається використання зовнішньої системи, умови якої передбачають невинуватене відчуження майнових прав на службові матеріали, використання службових матеріалів для навчання комерційних моделей без дозволу Верховного Суду, неконтрольоване передання даних третім особам або невизначений порядок їх зберігання та видалення. Використання захищених даних для навчання або вдосконалення моделей не допускається в будь-якому разі.

15.6. Запити, результати та журнали подій зберігаються не довше, ніж це необхідно для визначеної службової, безпекової або контрольної мети, якщо інший строк не встановлено законом. Для кожного схваленого способу використання визначаються строки зберігання, порядок видалення, коло осіб із доступом та, за потреби, порядок резервного копіювання.

16. Кібербезпекові вимоги

16.1. Під час упровадження та використання систем ШІ враховуються, зокрема, такі загрози:

16.1.1. несанкціонований доступ і витік даних;

16.1.2. приховані або шкідливі інструкції у документах, вебсторінках чи інших вхідних даних, спрямовані на зміну поведінки системи або обхід установлених обмежень;

16.1.3. навмисне спотворення, підміна або забруднення даних і джерел, що використовуються системою;

16.1.4. підміна або несанкціонована зміна результатів роботи системи;

16.1.5. розкриття службової інформації через журнали подій, службові повідомлення, канали зворотного зв'язку або зовнішні складові системи;

16.1.6. ризики, пов'язані з оновленнями, підключенням зовнішніх служб та автономним виконанням дій.

16.2. Для способів використання середнього та високого ризику визначаються щонайменше:

16.2.1. порядок автентифікації користувачів та розмежування доступу;

16.2.2. правила введення, завантаження та передання даних;

16.2.3. ведення журналів подій у необхідному та пропорційному обсязі;

16.2.4. порядок перевірки оновлень, зовнішніх складових і підключень до інших інформаційних систем;

16.2.5. порядок зберігання, видалення, резервного копіювання та відновлення даних;

16.2.6. порядок реагування на збої, підозрілі результати та інциденти;

16.2.7. можливість негайного обмеження доступу або припинення роботи системи.

17. Постачальники, санкції та юрисдикційні ризики

17.1. Не допускається використання системи, якщо неможливо встановити її постачальника, основні умови обробки даних, порядок доступу третіх осіб або правовий режим зберігання даних у межах, необхідних для оцінки безпеки.

17.2. Забороняється використання системи ШІ, якщо її постачальником, власником або особою, яка здійснює вирішальний вплив на такого постачальника чи власника, є держава-агресор або держава-окупант, її державний орган, юридична особа, створена відповідно до законодавства такої держави або зареєстрована на її території, фізична особа – громадянин або резидент такої держави, або інша особа, щодо якої законодавством України встановлено заборону відповідного використання. Така заборона застосовується також, якщо ключова інфраструктура системи розміщена на території держави-агресора або держави-окупанта.

17.3. Якщо щодо постачальника, власника, контролера, бенефіціарного власника системи або пов'язаних із нею осіб застосовано санкції, можливість використання системи визначається відповідно до змісту та обсягу відповідних санкцій і вимог законодавства України.

17.4. В інших випадках ризик доступу іноземної держави до службової інформації оцінюється з урахуванням юрисдикції постачальника і місця обробки даних, застосовного законодавства, договірних та технічних гарантій, категорій даних, а також рекомендацій Державної служби спеціального зв'язку та захисту інформації України й інших уповноважених органів у сфері кібербезпеки. Сам факт використання іноземної хмарної інфраструктури не є достатньою підставою для заборони.

Розділ IV. Оцінювання ризику, схвалення та Реєстр

18. Рівні ризику способу використання системи ШІ

18.1. Ризик оцінюється щодо конкретного способу використання системи ШІ з урахуванням службової мети, категорій даних, рівня автономності, технічного середовища, можливого впливу на права осіб, інтереси правосуддя, незалежність суддів та інформаційну безпеку.

18.2. До використання низького ризику належать технічні, мовні, довідкові або навчальні завдання, які не створюють юридично значущого змісту і не впливають на права чи обов'язки осіб.

18.3. До використання середнього ризику належать, зокрема, підготовка попередніх аналітичних матеріалів, узагальнення відкритої судової практики, опрацювання великих масивів відкритої інформації, підготовка зовнішніх інформаційних матеріалів та інші завдання, у яких результат системи ШІ може істотно вплинути на зміст службового матеріалу.

18.4. До використання високого ризику належать способи, що передбачають змістовне опрацювання захищених даних, крім суто технічних операцій, дозволених відповідно до пункту 10.2 цього Положення, роботу в критичних або важливих інформаційних системах, автономне виконання дій, істотний вплив на управлінські процеси або можливий вплив на права, інтереси чи правове становище осіб.

18.5. Заборонений цим Положенням спосіб використання не може бути схвалений незалежно від оціненого рівня ризику.

19. Реєстр схвалених способів використання систем ШІ

19.1. В Апараті Верховного Суду ведеться Реєстр схвалених способів використання систем ШІ.

19.2. У Реєстрі зазначаються щонайменше відомості, визначені Додатком 3.

19.3. Реєстр веде уповноважений структурний підрозділ. Порядок ведення Реєстру та рівні доступу до нього затверджує керівник Апарату Верховного Суду.

20. Схвалення та повторна оцінка

20.1. Без окремого схвалення допускаються лише способи використання, прямо визначені цим Положенням і Додатком 1 як такі, що не потребують схвалення.

20.2. Інші способи використання допускаються після їх схвалення керівником Апарату Верховного Суду за поданням уповноваженого структурного підрозділу та внесення до Реєстру.

20.3. Якщо спосіб використання стосується підготовки справ до розгляду працівниками патронатної служби, загальні умови такого використання схвалюються після погодження з Головою Верховного Суду, а застосування у конкретній справі здійснюється лише за дорученням відповідного судді.

20.4. За результатами оцінки може бути прийнято рішення:

20.4.1. дозволити використання у визначених межах;

20.4.2. дозволити використання з додатковими обмеженнями або заходами захисту;

20.4.3. дозволити дослідне використання на визначений строк та для визначеного кола користувачів;

20.4.4. відмовити у схваленні;

20.4.5. призупинити або припинити раніше схвалене використання.

20.5. Перед схваленням оцінюються мета, функції системи, категорії даних, умови їх зберігання і передання, доступ третіх осіб, можливість використання даних для навчання моделі, умови договору або правил користування, заходи кібербезпеки, ризику помилок і упередженості, можливість припинення використання, а для високого ризику — також вплив на права людини.

20.6. Для способів використання високого ризику до схвалення перевіряється стійкість системи до помилкових, маніпулятивних і шкідливих вхідних даних, спроб обходу встановлених обмежень

та несанкціонованого доступу, зокрема з урахуванням результатів тестування, проведеного постачальником, незалежною організацією або уповноваженим структурним підрозділом.

20.7. Істотна зміна моделі, функцій, умов обробки даних, технічного середовища, категорій користувачів або рівня ризику є підставою для повторної оцінки. До її завершення використання може бути обмежено або призупинено.

Розділ V. Моніторинг, аудит та інциденти

21. Моніторинг і аудит

21.1. Моніторинг використання схвалених систем ШІ здійснюється лише для забезпечення безпеки, перевірки дотримання цього Положення, оцінки роботи систем і реагування на інциденти.

21.2. Моніторинг не може використовуватися як прихований засіб оцінювання продуктивності, поведінки або професійних якостей працівників чи суддів.

21.3. Працівники мають бути поінформовані про мету ведення журналів подій, категорії даних, строки їх зберігання, коло осіб із доступом та порядок використання відповідної інформації.

21.4. Використання систем ШІ може бути предметом внутрішнього аудиту, за результатами якого можуть бути змінені умови схвалення, призупинено або припинено використання системи, а також визначено додаткові заходи захисту чи навчання.

22. Інциденти

22.1. Працівник невідкладно повідомляє безпосереднього керівника та уповноважений структурний підрозділ про інцидент або обґрунтовану підозру на інцидент.

22.2. До первинних заходів реагування можуть належати припинення або призупинення використання системи, обмеження доступу, фіксація обставин, оцінка можливого витоку чи неправомірної обробки даних, виправлення недостовірної інформації та повідомлення відповідальних підрозділів.

22.3. Порядок реагування на інциденти, строки повідомлення, відповідальні особи та правила документування затверджує керівник Апарату Верховного Суду. Первинні дії працівника визначені Додатком 4.

Розділ VI. Навчання, відкритість, відповідальність, перегляд і набрання чинності

23. Навчання працівників

23.1. Працівники, які використовують або можуть використовувати системи ШІ у службовій діяльності, проходять періодичне навчання або інструктаж, що організовуються Верховним Судом, зокрема у співпраці з Національною школою суддів України.

23.2. Навчання охоплює правила цього Положення, основні можливості та обмеження систем ШІ, захист даних, перевірку результатів за першоджерелами, безпечне формулювання запитів, ознаки недостовірних результатів, ризику надмірної довіри до автоматизованих результатів і схильності систем ШІ підлаштовувати відповідь під очікування користувача, кібербезпекові загрози, порядок фіксації істотного використання та реагування на інциденти.

24. Відкритість інформації про використання систем ШІ

24.1. За результатами моніторингу та аудиту Апарат Верховного Суду не рідше одного разу на рік готує та оприлюднює на офіційному вебсайті Верховного Суду узагальнений звіт про використання систем ШІ, який містить інформацію про напрями використання, схвалені способи

використання, результати застосування, ефективність, виявлені ризики, вжиті заходи безпеки, проведене навчання та узагальнені відомості про інциденти.

24.2. Звіт не може містити інформацію з обмеженим доступом, персональні дані, відомості про технічні вразливості та інші відомості, оприлюднення яких може створити загрозу безпеці Верховного Суду.

24.3. Оприлюднення інформації про використання систем ШІ не повинно створювати хибного уявлення про можливість використання систем ШІ для формування судових рішень або заміни суддівського розсуду.

24.4. Це Положення може бути предметом консультацій із суддями, науковцями, представниками адвокатури, фахівцями у сфері інформаційної безпеки, захисту персональних даних і штучного інтелекту та громадськістю.

25. Відповідальність

25.1. Порушення вимог цього Положення може враховуватися під час вирішення питання про відповідальність лише у випадках і порядку, встановлених законом, з урахуванням правового статусу відповідного працівника.

25.2. Під час оцінки дій працівника враховуються характер і наслідки порушення, форма вини, службові обов'язки, факт своєчасного повідомлення про інцидент та вжиті заходи для запобігання або усунення шкоди.

26. Перегляд, додатки та набрання чинності

26.1. Положення підлягає періодичному перегляду з урахуванням змін законодавства, розвитку технологій, міжнародних стандартів, практики Верховного Суду, результатів моніторингу та інцидентів.

26.2. Під час перегляду цього Положення враховуються документи, зазначені в пункті 2.2 цього Положення, а також нові документи Ради Європи, Європейської комісії з питань ефективності правосуддя, Європейського Союзу, ЮНЕСКО та уповноважених органів України у сфері штучного інтелекту і правосуддя.

26.3. Додатки 1–4 є невід'ємною частиною цього Положення. У разі розбіжності між текстом Положення та додатком застосовується текст Положення.

26.4. Це Положення затверджується наказом керівника Апарату Верховного Суду після погодження з Головою Верховного Суду та набирає чинності з дня, визначеного таким наказом.

26.5. У строк, визначений наказом про затвердження цього Положення, уповноважений структурний підрозділ проводить інвентаризацію систем ШІ, що фактично використовуються в Апараті Верховного Суду, та забезпечує оцінку відповідних способів використання, їх внесення до Реєстру або підготовку пропозицій щодо припинення використання. Технології ШІ, затверджені керівником Апарату Верховного Суду відповідно до підпункту 3 пункту 2 розділу IV Положення, затвердженого наказом керівника Апарату Верховного Суду від 08 грудня 2025 року № 117, підлягають першочерговому оцінюванню відповідно до цього Положення під час інвентаризації.

26.6. До завершення інвентаризації:

26.6.1. загальнодоступні системи можуть використовуватися лише для способів низького ризику з відкритою інформацією;

26.6.2. технології ШІ, затверджені відповідно до підпункту 3 пункту 2 розділу IV Положення, затвердженого наказом керівника Апарату Верховного Суду від 08 грудня 2025 року № 117, можуть використовуватися в межах і на умовах, визначених рішенням про їх затвердження, до завершення їх оцінювання, але не довше строку інвентаризації;

26.6.3. інші наявні корпоративні системи можуть тимчасово використовуватися в межах чинних договорів і налаштувань лише для способів низького ризику та без обробки захищених даних;

26.6.4. вбудовані офісні функції можуть використовуватися відповідно до пункту 10.2 цього Положення;

26.6.5. інші способи використання середнього і високого ризику допускаються лише після схвалення відповідно до цього Положення.

Додаток 1. Матриця допустимості використання систем ШІ

Матриця застосовується разом із текстом Положення. Позначення «після схвалення» означає схвалення конкретного способу використання та внесення його до Реєстру.

Вид даних або завдання	Загальнодоступна система	Корпоративна / хмарна система	Локальна захищена система	Вбудована офісна функція
Перевірка правопису, форматування відкритого тексту	дозволено	дозволено	дозволено	дозволено
Інші способи низького ризику з відкритою інформацією (Додаток 2, пункт 1)	дозволено	дозволено	дозволено	дозволено
Аналітичне узагальнення відкритої судової практики	після схвалення	після схвалення	після схвалення	після схвалення, якщо функція істотно впливає на зміст
Відкриті персональні дані та номери оприлюднених справ	лише за службовою потребою та в мінімальному обсязі	відповідно до схваленого способу	відповідно до схваленого способу	лише якщо дані не передаються за межі дозволеного середовища
Внутрішній службовий документ інформації обмеженим доступом без з	заборонено	після схвалення	після схвалення	дозволено лише за умов пункту 10.2

Вид даних або завдання	Загальнодоступна система	Корпоративна / хмарна система	Локальна захищена система	Вбудована офісна функція
Персональні дані, що не є правомірно оприлюдненими	заборонено	після схвалення за наявності правової підстави	після схвалення за наявності правової підстави	лише за умов пункту 10.2 та належного захисту
Непублічні матеріали судової справи	заборонено	після схвалення у захищеному середовищі	після схвалення	після схвалення, якщо функція обробляє зміст матеріалів справи
Відомості із закритого судового засідання	заборонено	заборонено	лише за умов пункту 7.9	лише якщо функція працює в локальному середовищі та дотримано вимог пунктів 7.9 і 10.2
Неоприлюднений проект судового рішення	заборонено	після схвалення за умовами пункту 7.7	після схвалення; технічні функції – за пунктом 10.2	дозволено для суто технічних операцій за пунктами 7.7 і 10.2
Відомості, що становлять таємницю ухвалення судового рішення	заборонено	заборонено	заборонено	заборонено
Автоматичне перетворення службової наради на текст	заборонено	після схвалення	після схвалення	після схвалення
Автоматизоване знеособлення судового рішення до оприлюднення	заборонено	після схвалення	після схвалення	після схвалення

Додаток 2. Типові способи використання за рівнем ризику

1. Низький ризик: перевірка правопису, форматування, попередній переклад відкритого тексту, технічне структурування, створення таблиць із відкритих даних, довідковий пошук у відкритих джерелах.

2. Середній ризик: узагальнення відкритої судової практики, підготовка попереднього аналітичного матеріалу, тематичне групування великих масивів відкритих джерел, підготовка зовнішнього інформаційного матеріалу з істотним використанням системи ШІ.

3. Високий ризик: опрацювання непублічних матеріалів справи, автоматизоване знеособлення рішень до оприлюднення, підключення до внутрішніх інформаційних систем, автономне виконання дій або змістовне опрацювання інших захищених даних, крім суто технічних операцій, дозволених відповідно до пункту 10.2 цього Положення.

4. Заборонене використання — будь-які способи використання систем ШІ, заборонені цим Положенням, зокрема передбачені пунктами 6, 9 і 12 цього Положення. До них належать, зокрема, прогнозування результату конкретної справи, формування правової позиції замість судді, автоматичне створення процесуальних актів, профілювання суддів, прихований або вибірковий відбір істотних доводів, обробка таємниці ухвалення судового рішення, втручання в автоматизований розподіл справ, приховане спостереження, розпізнавання емоцій, біометрична категоризація, а також створення оманливого синтетичного контенту.

Додаток 3. Мінімальні відомості Реєстру

1. назва системи та постачальник;
2. опис схваленого способу використання;
3. службова мета;
4. категорії користувачів;
5. категорії даних, які дозволено і заборонено обробляти;
6. технічне середовище;
7. рівень ризику та результати оцінювання і перевірок, проведених відповідно до пунктів 17, 18, 20.5 і 20.6 цього Положення;
8. вид рішення, прийнятого відповідно до пункту 20.4 цього Положення;
9. у разі дослідного використання — строк такого використання та коло користувачів;
10. у випадках, передбачених пунктом 20.3 цього Положення, — відомості про погодження з Головою Верховного Суду;
11. обмеження та обов'язкові заходи захисту;
12. строки зберігання запитів, результатів і журналів подій;
13. уповноважений структурний підрозділ;
14. дата схвалення та дата наступного перегляду;
15. відомості про призупинення, припинення або повторну оцінку.

Додаток 4. Первинні дії у разі інциденту

1. припинити дію, що може погіршити наслідки інциденту;
2. невідкладно повідомити безпосереднього керівника та уповноважений структурний підрозділ;

3. якщо інцидент стосується матеріалів конкретної судової справи, невідкладно повідомити суддю, у провадженні якого перебуває справа, або іншого суддю відповідного складу суду, визначеного внутрішнім порядком;
4. зафіксувати час, систему, характер даних і відомі обставини події;
5. не видаляти журнали подій або інші відомості, необхідні для перевірки, якщо їх збереження не збільшує ризик;
6. виконувати подальші вказівки уповноваженого структурного підрозділу щодо обмеження доступу, виправлення, повідомлення інших осіб або припинення використання системи.