МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УМАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Схвалено Вченою радою УНУ
(протокол від 29 липня 2026 р., № 16)

ЗАТВЕРДЖУЮ
В.о. ректора Уманського
національного університету

_____ Олена ЯРОШИНСЬКА
29.07.2026
Введено в дію наказом
від 29.07.2026 № 01-16/149/од

ПОЛІТИКА ВІДПОВІДАЛЬНОГО ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В УМАНСЬКОМУ НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ

Умань – 2026

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика відповідального впровадження та використання технологій штучного інтелекту в Уманському національному університеті (далі – Політика) визначає принципи, правила, організаційні механізми, права, обов'язки та обмеження щодо розроблення, придбання, налаштування, впровадження і використання технологій штучного інтелекту в освітній, науковій, науково-технічній, інноваційній, творчій, методичній, видавничій, експертній, конкурсній, адміністративній, управлінській та комунікаційній діяльності Уманського національного університету.

1.2. Метою Політики є створення в Уманському національному університеті (далі – Університет) умов для законного, етичного, безпечного, прозорого, педагогічно доцільного та результативного використання технологій штучного інтелекту із забезпеченням академічної доброчесності, прав і свобод людини, захисту персональних даних, інформаційної безпеки, справедливості, інклюзивності та реального людського контролю.

1.3. Політику розроблено відповідно до Конституції України, Закону України «Про академічну доброчесність» від 18 грудня 2025 року № 4742-IX, законів України «Про освіту» від 5 вересня 2017 року № 2145-VIII, «Про вищу освіту» від 1 липня 2014 року № 1556-VII, «Про наукову і науково-технічну діяльність» від 26 листопада 2015 року № 848-VIII, «Про авторське право і суміжні права» від 1 грудня 2022 року № 2811-IX, «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, «Про інформацію» від 2 жовтня 1992 року № 2657-XII, «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР, «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, розпорядження Кабінету Міністрів України від 2 грудня 2020 року № 1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні», розпорядження Кабінету Міністрів України від 9 травня 2025

року № 457-р «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки», інших актів законодавства України, Статуту Університету та локальних нормативних актів Університету.

1.4. Під час розроблення Політики враховано Рекомендації щодо відповідального використання штучного інтелекту у вищій освіті, підготовлені Міністерством освіти і науки України та Міністерством цифрової трансформації України, а також європейські ризик-орієнтовані підходи до регулювання систем штучного інтелекту. Такі рекомендації та підходи застосовуються як методичні орієнтири у частині, що не суперечить законодавству України.

1.5. Політика є спеціальним локальним нормативним актом Університету та складовою внутрішньої системи забезпечення якості освіти, системи забезпечення академічної доброчесності, системи захисту інформації та цифрового управління Університету.

1.6. Політика деталізує застосування в Університеті загальних засад використання технологій штучного інтелекту, визначених Положенням про систему забезпечення академічної доброчесності в Уманському національному університеті. Процедура встановлення порушень академічної доброчесності, застосування заходів реагування та оскарження рішень регулюється Порядком подання та розгляду повідомлень про порушення академічної доброчесності, застосування заходів реагування та оскарження рішень в Уманському національному університеті.

1.7. Політика не встановлює загальної заборони на використання технологій штучного інтелекту. Використання таких технологій допускається за умови дотримання законодавства, вимог цієї Політики, правил конкретної діяльності, умов навчального завдання, наукового дослідження, конкурсу, експертизи або адміністративного процесу.

1.8. Використання технологій штучного інтелекту не звільняє особу від відповідальності за достовірність, якість, законність, академічну доброчесність,

безпечність та наслідки результату, який вона створила, подала, оприлюднила, схвалила, підписала або використала.

1.9. Остаточні рішення, що безпосередньо впливають на права, обов'язки, академічний статус, оцінювання, вступ, відрахування, працевлаштування, дисциплінарну відповідальність або доступ особи до можливостей Університету, не можуть прийматися виключно системою штучного інтелекту без змістовного розгляду і рішення уповноваженої людини.

1.10. У разі суперечності між Політикою та актом законодавства України застосовується акт законодавства України. У разі зміни законодавства окремі положення Політики застосовуються в частині, що не суперечить акту вищої юридичної сили, до приведення Політики у відповідність.

2. ОСНОВНІ ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

2.1. У цій Політиці терміни вживаються у таких значеннях:

2.1.1. Штучний інтелект – інформаційні (комп'ютерні) системи чи програми, здатні на основі опрацювання даних генерувати тексти, зображення, аудіовізуальні матеріали, програмний код, моделі, дані чи інші результати або виконувати завдання, що потребують інтелектуальної діяльності людини.

2.1.2. Система штучного інтелекту – програмний, програмно-апаратний або хмарний засіб, що реалізує функції штучного інтелекту та використовується самостійно або як складова іншої інформаційної системи.

2.1.3. Генеративний штучний інтелект – технологія штучного інтелекту, призначена для створення нового текстового, графічного, аудіовізуального, програмного, модельного чи іншого цифрового результату на підставі запиту користувача та опрацьованих моделлю даних.

2.1.4. Результат, згенерований технологіями штучного інтелекту – текст, зображення, аудіо-, відеоматеріал, програмний код, модель, набір даних,

аналітичний висновок, переклад, структура, рекомендація або інший результат, повністю чи частково створений системою штучного інтелекту.

2.1.5. Промпт – текстова, голосова, візуальна, програмна або інша інструкція, запит чи набір вхідних даних, що надаються системі штучного інтелекту для отримання результату.

2.1.6. Суттєве використання технологій штучного інтелекту – використання, яке істотно вплинуло на зміст, структуру, аргументацію, висновки, дані, програмний код, зображення, методику або іншу змістову частину результату діяльності та виходить за межі суто технічної допомоги.

2.1.7. Технічне використання технологій штучного інтелекту – використання для перевірки правопису, форматування, транскрибування власного мовлення, перетворення формату, забезпечення доступності або інших операцій, що не створюють і не змінюють змістовий внесок особи.

2.1.8. Декларація використання технологій штучного інтелекту – повідомлення особи про факт, мету, інструмент, обсяг і спосіб використання технологій штучного інтелекту під час створення конкретного результату.

2.1.9. Людський контроль – організаційні та технічні заходи, що забезпечують можливість компетентної людини розуміти призначення і межі системи, перевіряти її результат, втручатися в процес, не погоджуватися з рекомендацією, виправляти або припиняти використання системи.

2.1.10. Рішення істотного впливу – рішення, здатне суттєво вплинути на права, обов’язки, академічний чи трудовий статус, оцінювання, вступ, фінансування, доступ до освіти, роботи, стипендії, гранту, мобільності або іншої значущої можливості.

2.1.11. Схвалена система штучного інтелекту – система, офіційне впровадження або використання якої в Університеті погоджено у встановленому цією Політикою порядку та внесено до реєстру схвалених систем.

2.1.12. Зовнішня система штучного інтелекту – система, що функціонує поза інформаційною інфраструктурою Університету та надається стороннім постачальником, зокрема через вебсервіс, мобільний застосунок або програмний інтерфейс.

2.1.13. Система високого ризику – система, використання якої може істотно впливати на права та можливості осіб, безпеку, персональні дані, академічний або трудовий статус, або передбачає масштабну чи систематичну обробку чутливої інформації.

2.1.14. Синтетичний контент – матеріал, штучно створений або істотно змінений системою штучного інтелекту таким чином, що він може сприйматися як справжній запис події, голосу, зображення чи дій реальної особи.

2.1.15. Детектор використання штучного інтелекту – програмний засіб, який прогнозує імовірність того, що текст або інший матеріал створено чи змінено за допомогою технологій штучного інтелекту.

2.1.16. Інцидент, пов’язаний із технологіями штучного інтелекту – подія, що призвела або могла призвести до порушення прав особи, витоку чи неправомірної обробки даних, дискримінаційного результату, істотної помилки, порушення академічної доброчесності, інформаційної безпеки або іншої шкоди.

2.1.17. Паспорт системи штучного інтелекту – внутрішній документ, у якому фіксуються призначення, відповідальний підрозділ, постачальник, категорії користувачів і даних, рівень ризику, обмеження, заходи людського контролю, строки перегляду та інші відомості про офіційно впроваджену систему.

2.1.18. Недоброчесне використання результатів, згенерованих штучним інтелектом – порушення академічної доброчесності, зміст якого визначається Законом України «Про академічну доброчесність».

2.2. Терміни «академічна діяльність», «академічний твір», «навчальна робота», «персональні дані», «конфіденційна інформація», «службова інформація», «інформація з обмеженим доступом», «автор» та інші терміни вживаються у

значеннях, визначених законодавством України та локальними нормативними актами Університету.

3. МЕТА, ЗАВДАННЯ ТА ПРИНЦИПИ ПОЛІТИКИ

3.1. Основною метою Політики є забезпечення такого впровадження і використання технологій штучного інтелекту, за якого вони підсилюють навчання, викладання, дослідження, управління та доступність освіти, але не підміняють особисту інтелектуальну, творчу і професійну відповідальність людини.

3.2. Завданнями Політики є:

– визначення єдиних правил використання технологій штучного інтелекту учасниками діяльності Університету;
– запровадження ризик-орієнтованого підходу до вибору, придбання, впровадження та експлуатації систем штучного інтелекту;
– забезпечення прозорого декларування суттєвого використання штучного інтелекту в академічних творах, навчальних роботах та інших результатах діяльності;
– підтримка академічної доброчесності, авторства, достовірності даних і відтворюваності досліджень;
– захист персональних даних, інформації з обмеженим доступом та інформаційної інфраструктури Університету;
– недопущення дискримінації, непрозорого профілювання та необґрунтованого автоматизованого прийняття рішень;
– забезпечення рівного доступу до технологій, альтернативних способів виконання завдань та інклюзивності;
– формування у здобувачів освіти і працівників компетентностей відповідального та критичного використання штучного інтелекту;

– визначення порядку повідомлення про інциденти, перегляду та припинення використання небезпечних або неналежних систем.

3.3. Впровадження і використання технологій штучного інтелекту ґрунтується на таких принципах:

– людиноцентризм і повага до людської гідності;

– законність та дотримання прав і свобод людини;

– академічна доброчесність і персональна відповідальність;

– реальний людський контроль та можливість перегляду автоматизованого результату;

– прозорість, пояснюваність у межах технічної можливості та належне декларування;

– перевірка достовірності, точності, джерел і обмежень отриманого результату;

– справедливість, недискримінація та запобігання алгоритмічним упередженням;

– мінімізація обсягу даних та обмеження мети їх обробки;

– конфіденційність, інформаційна безпека та кіберстійкість;

– доступність, інклюзивність і недопущення цифрової нерівності;

– пропорційність технологічного рішення меті та рівню ризику;

– підзвітність осіб і підрозділів, які впроваджують або використовують системи;

– регулярний моніторинг, перегляд і вдосконалення практик.

3.4. Використання системи штучного інтелекту допускається лише тоді, коли очікувана користь обґрунтовано переважає ризики, а ті самі цілі не можуть бути досягнуті менш ризиковим способом із порівнянними витратами та якістю.

4. СФЕРА ДІЇ ТА СУБ'ЄКТИ ПОЛІТИКИ

4.1. Дія Політики поширюється на здобувачів вищої освіти всіх рівнів і форм здобуття освіти, аспірантів, докторантів, педагогічних, науково-педагогічних, наукових та інших працівників Університету, вступників, членів екзаменаційних,

приймальних, конкурсних, редакційних, експертних та інших комісій, зовнішніх експертів, рецензентів, підрядників і партнерів у частині використання ними систем або інформаційних ресурсів Університету.

4.2. Політика застосовується до використання технологій штучного інтелекту на обладнанні Університету, через університетські облікові записи, у придбаних або інтегрованих Університетом системах, а також у будь-якій діяльності, результат якої подається, оприлюднюється чи використовується від імені Університету.

4.3. Дія Політики поширюється на індивідуальне використання загальнодоступних зовнішніх систем під час виконання навчальних, наукових або службових завдань, навіть якщо таке використання відбувається поза територією Університету та на особистому обладнанні.

4.4. Підрядники та постачальники, які отримують доступ до даних або систем Університету, зобов’язані дотримуватися вимог Політики в обсязі, визначеному договором, технічним завданням та законодавством.

4.5. Керівники структурних підрозділів забезпечують ознайомлення працівників і здобувачів освіти з вимогами Політики в частині, що стосується діяльності відповідного підрозділу.

4.6. Політика не обмежує використання спеціальних засобів доступності особами з інвалідністю або особливими освітніми потребами, якщо таке використання не змінює змістовий результат завдання або дозволене його умовами.

4.7. Спеціальні вимоги до використання технологій штучного інтелекту можуть установлюватися робочими програмами освітніх компонентів, умовами завдань, правилами наукового дослідження, видання, конкурсу, експертизи чи інформаційної системи. Такі вимоги не можуть суперечити Політиці та законодавству.

5. КЛАСИФІКАЦІЯ РИЗИКІВ ТА ЗАБОРОНЕНІ ПРАКТИКИ

5.1. Для цілей внутрішнього управління використання систем штучного інтелекту класифікується за рівнями мінімального, обмеженого та високого ризику. Окремо визначаються заборонені практики. Орієнтовна Матриця рівнів ризику наведена в Додатку А.

5.2. До мінімального ризику належить технічне або допоміжне використання, яке не формує рішення істотного впливу, не передбачає обробки інформації з обмеженим доступом і не замінює змістовну діяльність людини.

5.3. До обмеженого ризику належить створення, редагування, переклад, узагальнення, програмування, візуалізація, аналітична або консультаційна допомога, що може вплинути на зміст результату, але не використовується для самостійного прийняття рішення істотного впливу.

5.4. До високого ризику належать системи, що використовуються або плануються для:

– вступного відбору, оцінювання результатів навчання, атестації, визначення академічного прогресу або ризику відрахування;
– розподілу стипендій, грантів, місць академічної мобільності, матеріальної допомоги чи інших обмежених можливостей;
– добору, рейтингового оцінювання, атестації, просування, дисциплінарного провадження або припинення трудових відносин;
– біометричної ідентифікації, систематичного спостереження, профілювання або аналізу поведінки осіб;
– опрацювання значних масивів персональних, біометричних, медичних або інших чутливих даних;
– формування рекомендацій, від яких фактично залежить рішення істотного впливу;

– використання в критичних елементах інформаційної інфраструктури чи безпеки Університету.

5.5. Система високого ризику може бути впроваджена лише після документованого попереднього оцінювання, правової, інформаційно-безпекової та етичної перевірки, визначення відповідальних осіб, способу людського контролю, порядку оскарження результату та рішення ректора або уповноваженої ним особи.

5.6. В Університеті забороняється:

– приймати остаточне рішення істотного впливу виключно на підставі автоматизованого висновку без змістовного людського розгляду;
– використовувати приховані маніпулятивні методи, спрямовані на істотне спотворення поведінки особи та завдання їй шкоди;
– здійснювати соціальне рейтингування здобувачів освіти або працівників за даними, не пов’язаними безпосередньо з легітимною метою оцінювання;
– визначати емоційний стан здобувачів освіти чи працівників за голосом, обличчям або поведінкою, крім належно обґрунтованих випадків охорони здоров’я або безпеки, прямо дозволених законом;
– здійснювати біометричну категоризацію за ознаками, що розкривають чутливі персональні характеристики, якщо це не передбачено законом;
– створювати або поширювати синтетичні аудіо-, відео- чи фотоматеріали, що імітують реальну особу, без законної підстави, згоди у випадках, коли вона необхідна, та чіткого маркування;
– використовувати технології штучного інтелекту для фабрикації або фальсифікації даних, джерел, цитувань, респондентів, експериментів чи результатів дослідження;
– використовувати технології штучного інтелекту для обходу правил оцінювання, автентифікації, інформаційної безпеки або контролю академічної доброчесності;

– завантажувати персональні дані, службову, конфіденційну або іншу інформацію з обмеженим доступом до несхвалених зовнішніх систем;
– застосовувати систему, про відомі критичні вразливості, дискримінаційні властивості або істотну недостовірність якої не вжито належних заходів реагування.

5.7. Якщо конкретне використання не можна однозначно віднести до рівня ризику, воно попередньо класифікується за вищим із можливих рівнів до завершення оцінювання.

5.8. Класифікація системи переглядається у разі зміни її призначення, функціональності, постачальника, категорій даних, масштабу використання або можливих наслідків.

6. УПРАВЛІННЯ ТА РОЗПОДІЛ ПОВНОВАЖЕНЬ

6.1. Вчена рада Університету:
– визначає основні напрями політики Університету у сфері штучного інтелекту;
– схвалює цю Політику та зміни до неї;
– розглядає узагальнені звіти про впровадження технологій штучного інтелекту та ухвалює рішення щодо вдосконалення відповідних практик.

6.2. Ректор Університету:
– забезпечує реалізацію Політики;
– утворює Координаційну групу з питань відповідального використання технологій штучного інтелекту (далі – Координаційна група) та затверджує її склад;
– приймає рішення про офіційне впровадження систем високого ризику, затвердження реєстру схвалених систем та припинення використання системи;
– забезпечує необхідні організаційні, фінансові, технічні та кадрові ресурси.

6.3. Координаційна група є консультативно-дорадчим органом, який:

– розглядає пропозиції щодо придбання, інтеграції та використання систем штучного інтелекту;
– проводить або організовує попереднє оцінювання ризиків;
– готує рекомендації щодо рівня ризику, умов використання, людського контролю та заходів захисту;
– веде або координує ведення реєстру схвалених систем і паспортів систем;
– аналізує інциденти та готує пропозиції щодо їх усунення;
– готує методичні матеріали та пропозиції до щорічного звіту.

6.4. До складу Координаційної групи включаються представники керівництва, відділу моніторингу якості освіти, юридичного, інформаційно-обчислювального центру, наукового відділу, бібліотеки, органів студентського самоврядування і Наукового товариства студентів, аспірантів, докторантів і молодих вчених. За потреби залучаються інші фахівці без права вирішального голосу.

6.5. Координаційна група не встановлює фактів порушення академічної доброчесності та не підміняє Комісію з питань академічної доброчесності.

6.6. Відділ моніторингу якості освіти:
– координує моніторинг використання технологій штучного інтелекту в освітньому процесі;
– збирає узагальнені дані про режими використання, декларування і типові ризики;
– організовує опитування та готує пропозиції щодо вдосконалення освітніх практик.

6.7. Інформаційно-обчислювальний центр:
– оцінює технічну сумісність, безпеку, кіберстійкість, керування доступом, журналювання і можливість резервного копіювання;
– забезпечує технічне впровадження схвалених систем;
– вживає заходів з локалізації інцидентів та припинення несанкціонованого доступу.

6.8. Юридичний відділ здійснює правову експертизу договорів, умов використання, правових підстав обробки даних, авторсько-правових питань та проєктів локальних актів у сфері штучного інтелекту.

6.9. Науковий відділ координує вимоги до використання технологій штучного інтелекту в дослідженнях, наукових проєктах, публікаціях та роботі з дослідницькими даними.

6.10. Бібліотека здійснює інформаційну і консультаційну підтримку щодо перевірки джерел, бібліографічних посилань, авторського права, інформаційної грамотності та відповідального використання генеративних систем.

6.11. Керівники структурних підрозділів визначають відповідальних осіб за офіційно впроваджені системи, контролюють дотримання умов їх використання та невідкладно повідомляють про інциденти.

6.12. Кожен користувач несе персональну відповідальність за дотримання Політики, правил доступу, умов завдання, достовірність введених даних і перевірку використаного результату.

7. ОЦІНЮВАННЯ, СХВАЛЕННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

7.1. Придбання, підписка, інтеграція з інформаційними системами Університету, масове розгортання або офіційне використання системи штучного інтелекту здійснюється лише після попереднього оцінювання.

7.2. Ініціатор впровадження подає Координаційній групі заявку за формою Додатка Г, у якій зазначає мету, очікувану користь, категорії користувачів, даних, можливих рішень, постачальника, спосіб інтеграції, необхідні ресурси та відомі обмеження.

7.3. Під час оцінювання перевіряються: законність мети; пропорційність; рівень ризику; види і походження даних; правова підстава їх обробки; умови зберігання і

передання; використання даних постачальником для навчання моделі; точність; відомі обмеження; можливість пояснення; ризик дискримінації; доступність; кібербезпека; авторські права; можливість людського втручання; порядок оскарження; умови припинення використання.

7.4. Для систем високого ризику обов’язково визначаються відповідальна посадова особа, компетентні користувачі, процедура перевірки результату, журналювання рішень, строки повторного оцінювання, порядок повідомлення особи про використання системи та можливість звернутися за людським переглядом.

7.5. За результатами оцінювання Координаційна група рекомендує: схвалити систему без додаткових умов; схвалити з обмеженнями; провести пілотне використання; повернути на доопрацювання; відмовити у впровадженні.

7.6. Рішення про впровадження систем ШІ приймає Вчена рада Університету.

7.7. Для кожної офіційно впровадженої системи оформлюється паспорт за формою Додатка Ґ та визначається дата наступного перегляду.

7.8. Реєстр схвалених систем містить назву, постачальника, призначення, відповідальний підрозділ, рівень ризику, категорії дозволених даних, основні обмеження та строк перегляду. Відомості, розкриття яких створює ризик безпеці, не оприлюднюються.

7.9. Індивідуальне використання загальнодоступної системи для завдань мінімального або обмеженого ризику не потребує внесення до реєстру, якщо користувач не вводить інформацію з обмеженим доступом, не здійснює інтеграцію з університетськими системами та дотримується цієї Політики.

7.10. Істотна зміна функціональності, призначення, умов постачальника, переліку даних або масштабу використання є підставою для повторного оцінювання.

7.11. Договори з постачальниками мають, наскільки це можливо, визначати права на введені дані і результати, заборону неузгодженого використання даних

для навчання моделей, строки зберігання, місце обробки, заходи безпеки, порядок повідомлення про витік, видалення даних, аудит і припинення послуги.

7.12. Використання безоплатної версії сервісу не звільняє користувача і підрозділ від оцінювання умов конфіденційності, ліцензії, способу використання даних та інших ризиків.

8. ЗАГАЛЬНІ ПРАВИЛА КОРИСТУВАННЯ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ

8.1. Користувач застосовує систему лише для законної мети та в межах наданих повноважень, умов доступу, навчального завдання, трудових обов’язків або дослідницького протоколу.

8.2. До введення даних користувач визначає їх категорію та переконується, що передання таких даних відповідній системі дозволене.

8.3. Користувач не повинен вважати результат системи достовірним лише з огляду на його переконливу форму. Факти, обчислення, джерела, цитати, правові посилання, програмний код і висновки підлягають перевірці за незалежними та надійними джерелами.

8.4. Користувач повинен враховувати можливість вигаданих фактів, неіснуючих джерел, застарілих відомостей, прихованих упереджень, неправильної інтерпретації контексту, небезпечного коду та інших помилок.

8.5. Забороняється передавати іншій особі університетський обліковий запис, ключ програмного інтерфейсу або інші засоби доступу до системи.

8.6. Не допускається навмисне формування запитів, спрямованих на отримання протиправного, дискримінаційного, оманливого або такого, що порушує права інших осіб, результату.

8.7. Результат системи використовується лише після змістовного перегляду, виправлення та адаптації компетентною людиною. Формальне копіювання результату без перевірки не вважається належним людським контролем.

8.8. За потреби забезпечення доказовості, відтворюваності або виконання умов завдання користувач зберігає промпти, проміжні результати, версії файлів, дату, назву і версію системи упродовж строку, визначеного відповідним актом чи завданням.

8.9. Якщо система надає рекомендацію, що може завдати шкоди, порушити права, спричинити істотну помилку або суперечить професійним знанням користувача, така рекомендація не застосовується до з'ясування обставин.

9. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЬОМУ ПРОЦЕСІ

9.1. Технології штучного інтелекту можуть використовуватися для персоналізації навчання, створення прикладів, моделювання, тренування навичок, зворотного зв'язку, доступності, перекладу, пошуку ідей, аналізу даних та інших педагогічно обґрунтованих цілей.

9.2. Використання технологій штучного інтелекту має відповідати результатам навчання та не повинно усувати необхідність формування в здобувача освіти знань, критичного мислення, самостійності, професійних, дослідницьких, комунікаційних і творчих компетентностей.

9.3. Викладач завчасно визначає режим використання технологій штучного інтелекту для кожного завдання, якщо характер завдання допускає різні підходи. Правило повідомляється до початку виконання через робочу програму, LMS, текст завдання або інший офіційний канал.

9.4. Якщо режим не визначено, здобувач має право звернутися за уточненням. Відсутність відповіді не означає автоматичної дозволеності використання, якщо метою завдання є оцінювання особистого результату без зовнішньої допомоги.

9.5. Викладач не може змінювати режим після подання роботи та застосовувати нові обмеження до вже виконаного завдання.

9.6. Завдання, що передбачає використання конкретного платного сервісу, допускається лише за умови надання Університетом доступу або рівноцінної безоплатної альтернативи.

9.7. Здобувачам мають надаватися зрозумілі приклади дозволеного і забороненого використання та вимоги до декларування.

9.8. Використання системи для пояснення матеріалу, тренування, генерації додаткових прикладів або самоперевірки не повинно підміняти офіційні навчальні матеріали та консультації викладача.

9.9. Під час використання чатботів або віртуальних помічників у навчанні користувачеві повідомляється, що він взаємодіє з автоматизованою системою, та надається спосіб звернення до людини у разі важливого або спірного питання.

9.10. Рекомендації системи щодо індивідуальної освітньої траєкторії мають допоміжний характер і не можуть автоматично обмежувати право здобувача на вибір, переведення, поновлення або іншу освітню можливість.

10. РЕЖИМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В НАВЧАЛЬНИХ ЗАВДАННЯХ

10.1. Для навчальних завдань установлюються такі режими:

– використання технологій штучного інтелекту заборонене;

– обмежене використання дозволене за умови дотримання визначених меж та декларування;

– використання дозволене або передбачене умовами завдання.

10.2. Режим заборони застосовується, якщо метою є перевірка особистих знань, мовлення, обчислювальних, творчих, професійних або інших компетентностей без змістовної допомоги генеративної системи.

10.3. За режиму заборони можуть дозволятися суто технічні та спеціальні засоби доступності, якщо викладач не визначив інше і вони не створюють змістової відповіді.

10.4. За режиму обмеженого використання викладач визначає дозволені функції, інструменти, етапи роботи, максимальний обсяг допомоги, форму декларації та необхідність подання промптів, чернеток або історії змін.

10.5. За режиму дозволеного або передбаченого використання оцінюється не лише кінцевий результат, а й здатність сформулювати завдання системі, критично перевірити результат, виявити помилки, обґрунтувати зміни та продемонструвати власний внесок.

10.6. Режим і приклади його формулювання наведено в Додатку Б.

10.7. Для групового завдання викладач визначає, чи є використання технологій штучного інтелекту частиною спільної роботи та як декларується внесок кожного учасника.

10.8. У кваліфікаційній, курсовій або іншій академічній роботі режим використання визначається законодавством, цією Політикою, методичними вказівками, доведеними до автора до офіційного подання.

10.9. Порушення режиму не кваліфікується автоматично без урахування змісту завдання, фактичного способу використання, особистого внеску, декларування, форми вини та сукупності доказів.

10.10. Якщо здобувач використав систему через об’єктивну потребу доступності, він має право повідомити про це викладача конфіденційно та отримати рівноцінні умови оцінювання.

11. ПРАВА ТА ОБОВ'ЯЗКИ ПЕДАГОГІЧНИХ, НАУКОВО-ПЕДАГОГІЧНИХ І НАУКОВИХ ПРАЦІВНИКІВ

11.1. Працівник має право використовувати технології штучного інтелекту для підготовки матеріалів, планування, аналізу, перекладу, програмування, візуалізації та інших професійних завдань у межах законодавства і Політики.

11.2. Працівник зобов'язаний:

– визначати і завчасно повідомляти правила використання технологій штучного інтелекту в навчальних завданнях;
– перевіряти матеріали, питання, відповіді, посилання, обчислення та інші результати, створені за допомогою системи;
– не завантажувати до несхваленої системи навчальні роботи, персональні дані, неопубліковані твори або матеріали з обмеженим доступом;
– не застосовувати автоматизований висновок як єдину підставу оцінки, звинувачення або рішення істотного впливу;
– забезпечувати здобувачеві можливість пояснити процес виконання роботи та надати докази власного внеску;
– декларувати суттєве використання технологій штучного інтелекту у власних академічних творах, навчальних матеріалах і професійних документах, якщо цього вимагає характер результату;
– враховувати доступність, фінансові та технічні можливості здобувачів;
– не перекладати на систему персональну відповідальність за оцінювання, науковий висновок, рецензію або службове рішення.

11.3. Викладач може вимагати усний захист, демонстрацію проміжних матеріалів, пояснення коду, методики або джерел, якщо це передбачено умовами завдання чи необхідно для перевірки досягнення результатів навчання. Такі заходи мають бути пропорційними та не використовуватися як покарання.

11.4. Працівник не повинен вимагати від здобувача передання паролів, повної історії особистого облікового запису або іншої надмірної інформації, не потрібної для перевірки конкретної роботи.

11.5. Створюючи матеріали за допомогою технологій штучного інтелекту, працівник перевіряє їх педагогічну доцільність, точність, відсутність дискримінаційних формулювань та відповідність віку і рівню підготовки здобувачів.

11.6. Застосування системи для підготовки зворотного зв'язку допускається лише за умови особистого перегляду і коригування такого зворотного зв'язку працівником.

11.7. Працівник має право отримувати методичну, правову та технічну консультацію щодо застосування Політики.

11.8. Негативні наслідки для працівника не можуть ґрунтуватися виключно на автоматизованій оцінці його діяльності.

12. ПРАВА ТА ОБОВ'ЯЗКИ ЗДОБУВАЧІВ ОСВІТИ

12.1. Здобувач освіти має право:

– знати режим використання технологій штучного інтелекту до початку виконання завдання;
– отримувати зрозумілі вимоги до декларування;
– користуватися дозволеними технологіями для навчання і розвитку компетентностей;
– отримати альтернативу у разі відсутності доступу до обов'язкового платного сервісу;
– отримувати консультації щодо відповідального використання;
– бути поінформованим про використання автоматизованих засобів під час оцінювання та вимагати людського перегляду істотного результату;

– надавати пояснення та докази власного внеску, якщо виникли сумніви щодо самостійності роботи.

12.2. Здобувач освіти зобов’язаний:

– дотримуватися режиму, установленого для конкретного завдання;

– декларувати суттєве використання технологій штучного інтелекту у визначеній формі;

– перевіряти достовірність фактів, обчислень, посилань, коду та інших результатів;

– бути здатним пояснити зміст поданої роботи, використану методику та власний внесок;

– не подавати повністю або суттєво згенерований результат як власний самостійний результат, якщо це заборонено правилами або не задекларовано;

– не використовувати вигадані системою джерела, дані, цитати чи результати;

– не вводити до зовнішніх систем персональні дані інших осіб, екзаменаційні матеріали, завдання з обмеженим доступом або іншу захищену інформацію;

– за потреби зберігати проміжні матеріали у строк, визначений завданням.

12.3. Використання технологій штучного інтелекту для пояснення, тренування або попередньої самоперевірки допускається, якщо воно не порушує умов завдання та не підміняє особистого виконання результату, що оцінюється.

12.4. Здобувач не зобов’язаний купувати підписку або передавати постачальнику більше персональних даних, ніж необхідно для виконання обов’язкового завдання.

12.5. Здобувач має право відмовитися від використання необов’язкової системи високого ризику та отримати рівноцінний спосіб виконання або оцінювання, якщо інше прямо не встановлено законом.

12.6. Особа не може бути визнана такою, що порушила академічну доброчесність, лише через незвичний стиль тексту, високий рівень мовної правильності або результат автоматизованого детектора.

12.7. Обов’язок доведення порушення не покладається на здобувача освіти. Водночас він добросовісно користується правом на пояснення та не подає завідомо неправдивих матеріалів.

12.8. Правила цього розділу застосовуються з урахуванням додаткових гарантій для неповнолітніх осіб та осіб з особливими освітніми потребами.

13. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ОЦІНЮВАННЯ

13.1. Системи штучного інтелекту можуть використовуватися для допоміжного створення завдань, попереднього аналізу відповідей, виявлення типових помилок, формування чернетки зворотного зв’язку або організаційної підтримки оцінювання.

13.2. Остаточну оцінку визначає викладач, екзаменаційна, атестаційна або інша уповноважена особа чи комісія, яка несе відповідальність за відповідність оцінки заздалегідь установленим критеріям.

13.3. Автоматизований результат підлягає змістовному перегляду. Виявлена системою помилка, збіг, аномалія або прогноз не є наперед установленим фактом.

13.4. Здобувачеві повідомляється про застосування системи штучного інтелекту, якщо її результат істотно використовується під час оцінювання або прийняття пов’язаного рішення.

13.5. Критерії оцінювання, порядок використання автоматизованих засобів і можливість людського перегляду мають бути доступними до проведення оцінювання в обсязі, достатньому для розуміння процедури.

13.6. Детектор використання штучного інтелекту не є самостійним і достатнім доказом недоброчесного використання результатів, згенерованих штучним інтелектом. Його результат може бути лише допоміжною інформацією та оцінюється разом з умовами завдання, декларуванням, змістом роботи, метаданими, проміжними матеріалами та поясненнями особи.

13.7. Не допускається встановлення універсального відсотка, за якого робота автоматично визнається створеною за допомогою штучного інтелекту або недоброчесною.

13.8. Якщо автоматизована система використовує персональні дані або формує профіль здобувача, її застосування здійснюється лише в схваленій системі та в мінімально необхідному обсязі.

13.9. Апеляція щодо оцінки розглядається людиною, яка має повноваження змінити результат і не обмежена автоматизованою рекомендацією.

13.10. Аудіо-, відеоспостереження, біометрична ідентифікація або інші засоби дистанційного контролю під час оцінювання застосовуються лише на законній підставі, пропорційно меті, з попереднім інформуванням і належним захистом даних.

14. ДЕКЛАРУВАННЯ ТА МАРКУВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

14.1. Суттєве використання технологій штучного інтелекту в академічному творі, навчальній роботі, науковому результаті, методичному матеріалі, експертному висновку або іншому результаті декларується, якщо інше прямо не визначено законом або правилами відповідної діяльності.

14.2. Декларація має бути достатньою для розуміння ролі системи та може містити назву системи, версію або дату використання, мету, етапи роботи, характер отриманої допомоги, обсяг згенерованого або перероблено матеріалу, спосіб перевірки та посилання на систему або її опис.

14.3. Орієнтовна форма декларації наведена в Додатку В. Вимоги конкретного видання, завдання, проєкту чи конкурсу можуть передбачати додаткові відомості.

14.4. У разі використання в академічному творі об’єкта, згенерованого штучним інтелектом, автор повідомляє про це із зазначенням методики генерування та/або посилання на відповідну програму чи її опис згідно з установленими вимогами.

14.5. Технічне використання для стандартної перевірки правопису, форматування, транскрибування власного мовлення, перетворення формату та забезпечення доступності не потребує окремої декларації, якщо воно не змінює зміст і викладач або правила видання не визначили інше.

14.6. Декларування не перетворює заборонене використання на дозволене та не звільняє особу від відповідальності за результат.

14.7. Синтетичний контент у публічній комунікації маркується у спосіб, доступний для звичайного користувача, якщо він може бути помилково сприйнятий як автентичний запис реальної події або особи.

14.8. Система штучного інтелекту не зазначається автором або співавтором. Відповідальність за академічний твір чи інший результат несуть фізичні особи.

14.9. Якщо правила видання або партнера встановлюють суворіші вимоги до декларування, застосовуються такі вимоги за умови їх попереднього доведення до автора.

15. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В НАУКОВІЙ І НАУКОВО-ТЕХНІЧНІЙ ДІЯЛЬНОСТІ

15.1. Технології штучного інтелекту можуть використовуватися для пошуку і систематизації інформації, аналізу даних, програмування, моделювання, візуалізації, перекладу, редагування, генерування гіпотез та інших дослідницьких завдань за умови наукової доброчесності і належного методологічного контролю.

15.2. Дослідник перевіряє реальне існування кожного використаного джерела, достовірність цитування, правильність обчислень, коду, моделей і висновків.

15.3. Забороняється використовувати систему для створення вигаданих первинних даних, респондентів, спостережень, експериментів, результатів або джерел і подавати їх як реальні.

15.4. Синтетичні дані можуть використовуватися лише як чітко позначений методологічний інструмент із описом способу їх створення, обмежень і відмінності від реальних даних.

15.5. Якщо використання системи є істотним для методики чи відтворюваності дослідження, у роботі зазначаються система, версія або дата доступу, параметри, основні промпти чи інший достатній опис процедури, а відповідні матеріали зберігаються в порядку управління дослідницькими даними.

15.6. Використання системи під час роботи з персональними, медичними, біометричними, геолокаційними або іншими чутливими даними допускається лише після визначення правової підстави, оцінювання ризиків та, за потреби, погодження відповідного етичного органу.

15.7. Неопубліковані рукописи, заявки, дисертації, рецензії, дані партнерів, комерційна таємниця або матеріали з договірними обмеженнями не вводяться до зовнішньої системи без дозволу правовласника, належної правової підстави та забезпечення конфіденційності.

15.8. Авторство визначається фактичним інтелектуальним і творчим внеском фізичних осіб. Система штучного інтелекту не може нести відповідальність, надавати згоду на публікацію або відповідати критеріям авторства.

15.9. Дослідник дотримується правил журналу, видавця, грантодавця або партнера щодо використання і декларування технологій штучного інтелекту.

15.10. У разі істотної залежності висновків від недоступної для перевірки закритої моделі дослідник розкриває це обмеження і, наскільки можливо, проводить незалежну валідацію.

15.11. Програмний код, створений за допомогою штучного інтелекту, перевіряється на функціональність, безпечність, наявність уразливостей, ліцензійні обмеження та можливе відтворення чужого коду.

15.12. Керівник наукового проєкту забезпечує включення правил використання технологій штучного інтелекту до плану управління даними або внутрішнього протоколу, якщо масштаб чи ризик використання цього потребує.

16. РЕЦЕНЗУВАННЯ, ЕКСПЕРТНА, РЕДАКЦІЙНА ТА КОНКУРСНА ДІЯЛЬНІСТЬ

16.1. Рецензент, експерт або член конкурсного органу не може передавати до зовнішньої системи неопублікований твір, заявку, дисертацію, проєкт, персональні дані або іншу конфіденційну інформацію без дозволу та законної підстави.

16.2. Використання штучного інтелекту для допоміжного мовного редагування, структурування власних нотаток або аналізу загальнодоступної інформації допускається, якщо не порушується конфіденційність та правила процедури.

16.3. Система не може підміняти професійне судження рецензента чи експерта. Висновок підписується людиною, яка особисто перевірила аргументи, джерела і несе відповідальність за зміст.

16.4. Суттєве використання технологій штучного інтелекту під час підготовки рецензії або експертного висновку декларується у такому документі, якщо це не розкриває захищену інформацію.

16.5. Не допускається автоматичне відхилення рукопису, заявки чи конкурсної пропозиції виключно на підставі автоматизованого прогнозу або детектора.

16.6. Редакції наукових видань Університету визначають у правилах для авторів і рецензентів вимоги до використання, декларування та перевірки матеріалів, створених за допомогою технологій штучного інтелекту.

16.7. Під час формування конкурсних рейтингів автоматизований інструмент може використовуватися лише як допоміжний засіб за умови прозорих критеріїв, перевірки людиною та врегулювання конфлікту інтересів.

16.8. Заявник або учасник конкурсу має бути повідомлений про істотне використання системи під час оцінювання та мати можливість оскаржити рішення до людини.

16.9. Не допускається використання системи для виявлення або прогнозування політичних, релігійних, етнічних, профспілкових, медичних чи інших чутливих характеристик учасника конкурсу.

16.10. Матеріали експертизи, промпти та результати системи зберігаються лише в необхідному обсязі та строк, якщо це потрібно для аудиту або оскарження.

17. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АДМІНІСТРАТИВНІЙ, УПРАВЛІНСЬКІЙ ТА КОМУНІКАЦІЙНІЙ ДІЯЛЬНОСТІ

17.1. Технології штучного інтелекту можуть використовуватися для підготовки чернеток документів, перекладу, класифікації звернень, пошуку інформації, планування, аналізу знеособлених даних, створення інформаційних матеріалів та інших допоміжних завдань.

17.2. Офіційний документ, лист, довідка, проєкт наказу, юридичний, фінансовий, кадровий або закупівельний матеріал підлягає професійній перевірці працівником до підписання або оприлюднення.

17.3. Система не має права самостійно видавати наказ, погоджувати платіж, укладати договір, приймати кадрове, дисциплінарне або інше управлінське рішення.

17.4. Під час автоматизованого сортування звернень має бути забезпечено, щоб важливе звернення не залишалося без людського розгляду через помилку класифікації.

17.5. Чатбот або інший автоматизований засіб комунікації чітко повідомляє користувачеві про автоматизований характер взаємодії та надає доступний спосіб звернення до працівника.

17.6. Відповідь чатбота не вважається офіційним рішенням Університету, якщо вона не підтверджена у встановленій формі уповноваженою особою.

17.7. Використання системи у кадровому доборі, рейтинговому оцінюванні або аналізі ефективності працівників належить до високого ризику та не може бути єдиною підставою відмови, пониження, дисциплінарного заходу або звільнення.

17.8. Працівникові або кандидатові повідомляється про істотне використання автоматизованої системи, критерії, які його стосуються, та можливість людського перегляду.

17.9. У публічних матеріалах не допускається створення синтетичних заяв, голосу або зображення керівника, працівника, здобувача чи іншої реальної особи без належної згоди, правової підстави і чіткого маркування.

17.10. Генеровані зображення, відео або інші матеріали не повинні вводити в оману щодо реальних приміщень, подій, обладнання, досягнень або осіб Університету.

17.11. Офіційні повідомлення, що можуть вплинути на безпеку, права, строки, вступ, оплату, оцінювання або трудові відносини, перевіряються людиною перед поширенням.

17.12. Використання технологій штучного інтелекту в закупівлях не звільняє відповідальну особу від перевірки технічних характеристик, ринкової інформації, законності вимог і відсутності дискримінаційних умов.

18. ПЕРСОНАЛЬНІ ДАНІ, КОНФІДЕНЦІЙНІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

18.1. Обробка персональних даних із використанням технологій штучного інтелекту здійснюється для визначеної законної мети, у мінімально необхідному обсязі, протягом обґрунтованого строку та з належним захистом.

18.2. До несхвалених зовнішніх систем забороняється вводити:

– паспортні, контактні, фінансові, медичні, біометричні та інші персональні дані;

– оцінки, результати навчання, матеріали особових справ, характеристики і дисциплінарні матеріали;

– логіни, паролі, ключі доступу, конфігурації та відомості про захист інформаційних систем;

– неопубліковані академічні твори, екзаменаційні завдання, службові документи, комерційну таємницю та іншу інформацію з обмеженим доступом;

– дані партнерів, використання яких обмежене договором або професійною таємницею.

18.3. До схваленої системи такі дані можуть вводитися лише в обсязі, передбаченому паспортом системи, за наявності правової підстави, належних умов договору, керування доступом та захисту.

18.4. За можливості дані знеособлюються, псевдонімізуються або замінюються тестовими даними до передання системі.

18.5. Користувач не надає системі доступ до електронної пошти, хмарного сховища, календаря, LMS чи іншого ресурсу понад обсяг, необхідний для конкретної мети.

18.6. Для систем високого ризику ведеться журнал доступу і ключових операцій у межах, необхідних для безпеки, аудиту та оскарження.

18.7. Перед використанням зовнішнього сервісу оцінюється, чи використовує постачальник введені дані для навчання моделей, кому їх передає, де зберігає, як довго утримує та чи надає можливість видалення.

18.8. Обробка даних неповнолітніх осіб потребує особливої обережності, мінімізації та застосування додаткових гарантій відповідно до законодавства.

18.9. Забороняється використовувати відкриту систему для генерування або аналізу інформації, розкриття якої може створити загрозу фізичній, інформаційній або кібербезпеці Університету чи окремої особи.

18.10. Результат системи перевіряється на наявність прихованого шкідливого коду, небезпечних інструкцій або витоку конфіденційної інформації до його використання в інформаційній інфраструктурі.

18.11. Під час інтеграції застосовуються принципи найменших привілеїв, багатофакторна автентифікація, розмежування доступу, оновлення, резервне копіювання і журналювання відповідно до рівня ризику.

18.12. Працівники та здобувачі невідкладно повідомляють про випадкове передання захищених даних, підозрілу активність, компрометацію облікового запису або інший інцидент.

18.13. Дані, промпти і результати видаляються після досягнення мети, якщо їх подальше зберігання не вимагається законом, договором, правилами дослідження, оскарження або архівування.

18.14. Право на доступ до інформації про роботу системи реалізується з урахуванням захисту комерційної таємниці, кібербезпеки та прав інших осіб, але не може використовуватися для приховування підстав рішення істотного впливу.

19. АВТОРСЬКЕ ПРАВО ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ

19.1. Використання технологій штучного інтелекту не скасовує обов’язку поважати авторські та суміжні права, права на бази даних, програмне забезпечення, торговельні марки та інші об’єкти інтелектуальної власності.

19.2. Користувач перевіряє, чи не відтворює результат системи істотні частини охоронюваного твору, програмного коду, зображення, музики або іншого об’єкта без належної правової підстави.

19.3. Використання чужого матеріалу, виявленого або перетвореного за допомогою системи, потребує посилання на першоджерело та автора, якщо цього вимагає закон або академічні правила.

19.4. Бібліографічне посилання, запропоноване системою, перевіряється за реально існуючим джерелом до включення в роботу.

19.5. Не допускається завантаження до системи чужого неопублікованого твору, рукопису, коду, зображення або іншого об’єкта без дозволу чи іншої законної підстави.

19.6. Під час закупівлі або інтеграції системи визначаються умови використання введених даних, право на отриманий результат, обмеження ліцензії та відповідальність сторін.

19.7. Система штучного інтелекту не зазначається автором або співавтором. Особа несе відповідальність за правомірність використання результату і достовірність заявленого авторства.

19.8. Якщо правовий статус конкретного згенерованого об’єкта є невизначеним, його використання у комерційному, видавничому або репутаційно значущому проєкті погоджується з юридичним відділом.

19.9. Порушення авторського права розглядається окремо від питання академічної доброчесності, якщо відповідні діяння мають різний предмет і правові підстави.

20. РІВНІСТЬ, НЕДИСКРИМІНАЦІЯ, ДОСТУПНІСТЬ ТА ІНКЛЮЗИВНІСТЬ

20.1. Університет уживає заходів для недопущення дискримінаційних або систематично упереджених результатів систем штучного інтелекту.

20.2. Система високого ризику до впровадження перевіряється на можливі необґрунтовані відмінності результатів щодо різних груп користувачів у межах, дозволених законом і методологічно можливих.

20.3. Дані, які не мають прямого зв’язку з легітимною метою оцінювання, не використовуються для прогнозування здібностей, надійності, доброчесності або професійної придатності особи.

20.4. Відсутність у здобувача освіти платної підписки, сучасного пристрою або високої цифрової компетентності не може сама по собі знижувати оцінку чи обмежувати освітню можливість.

20.5. Обов’язкове завдання з використанням системи передбачає інструкцію, навчання та рівноцінний доступ або альтернативу.

20.6. Засоби доступності, зокрема перетворення мовлення на текст, озвучення, спрощення навігації чи адаптація формату, підтримуються за умови збереження суті оцінюваної компетентності.

20.7. Користувач має право на зрозуміле пояснення істотного автоматизованого результату та його перегляд людиною.

20.8. У разі виявлення систематичного упередження використання системи обмежується або припиняється до усунення ризику.

21. ВИЯВЛЕННЯ ТА РОЗГЛЯД МОЖЛИВИХ ПОРУШЕНЬ

21.1. Факт використання технологій штучного інтелекту сам по собі не є порушенням академічної доброчесності.

21.2. Під час правової кваліфікації враховуються вид діяльності, режим і умови завдання, характер використання, обсяг особистого внеску, факт і повнота декларування, зміст результату, мета дій, форма вини та сукупність доказів.

21.3. Залежно від обставин неналежне використання може містити ознаки недоброчесного використання результатів, згенерованих штучним інтелектом,

несамостійного виконання завдання, недозволеної допомоги, академічного плагіату, фабрикації, фальсифікації або іншого порушення, визначеного законом.

21.4. Порушення правил захисту даних, інформаційної безпеки, авторського права або трудових обов’язків може розглядатися за відповідними окремими процедурами незалежно від наявності порушення академічної доброчесності.

21.5. Детектор використання штучного інтелекту, показник ймовірності, стиль тексту, відсутність помилок або суб’єктивне враження не є самостійним і достатнім доказом порушення.

21.6. До допоміжних доказів можуть належати умови завдання, декларація, метадані, історія версій, проміжні матеріали, пояснення особи, характер помилок, реальні джерела, експертний висновок та інші законно отримані відомості.

21.7. Відмова особи від пояснень або неможливість надати повну історію взаємодії із зовнішнім сервісом не вважається автоматичним визнанням порушення.

21.8. Повідомлення про можливе порушення академічної доброчесності подається і розглядається Комісією з питань академічної доброчесності відповідно до спеціального Порядку. Координаційна група може надавати технічні або методичні пояснення, але не встановлює вину.

21.9. Заходи реагування застосовуються лише після встановлення факту порушення і вини у встановленому порядку, крім прямих організаційних наслідків, передбачених законом або заздалегідь установленими правилами оцінювання.

22. ІНЦИДЕНТИ ТА ПРИПИНЕННЯ ВИКОРИСТАННЯ СИСТЕМИ

22.1. Про інцидент може повідомити будь-який користувач, працівник, здобувач освіти або інша особа, права якої можуть бути порушені. Орієнтовна форма повідомлення наведена в Додатку Д.

22.2. Повідомлення подається керівнику відповідного підрозділу, інформаційно-обчислювальному центру, Координаційній групі або через визначений Університетом канал. Повідомлення про витік чи кіберінцидент передається невідкладно.

22.3. До інцидентів належать витік даних, несанкціонований доступ, масове формування помилкових чи дискримінаційних результатів, порушення авторських прав, небезпечний код, приховане використання даних постачальником, відсутність можливості людського контролю та інші істотні відхилення.

22.4. Відповідальний підрозділ фіксує повідомлення, оцінює терміновість, уживає заходів для локалізації наслідків і збереження необхідних доказів.

22.5. У разі безпосереднього ризику система або окрема функція тимчасово блокується без очікування завершення повної перевірки. Таке блокування є запобіжним заходом, а не санкцією.

22.6. Координаційна група або визначена комісія аналізує причини, масштаб, постраждалі категорії даних та осіб, дії постачальника, достатність контролів і потребу в повідомленні компетентних органів або осіб.

22.7. За результатами можуть бути визначені коригувальні заходи, додаткове навчання, зміна параметрів, обмеження функцій, повторне оцінювання, зміна постачальника або повне припинення використання.

22.8. Особи, чиї права або дані могли бути істотно порушені, повідомляються у випадках і порядку, визначених законодавством.

22.9. Інформація про інциденти використовується для вдосконалення системи управління, але не оприлюднюється з необґрунтованим розкриттям персональних даних або відомостей, що створюють загрозу безпеці.

23. ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ, МОНІТОРИНГ І ЗВІТНІСТЬ

23.1. Університет організовує систематичне навчання здобувачів освіти і працівників з питань можливостей, обмежень, академічної доброчесності, перевірки фактів, захисту даних, авторського права, кібербезпеки та недискримінації під час використання технологій штучного інтелекту.

23.2. Новоприйняті працівники та здобувачі першого року навчання ознайомлюються з основними вимогами Політики в межах адаптаційних заходів.

23.3. Працівники, які використовують системи високого ризику, проходять спеціальну підготовку до отримання доступу та періодичне оновлення знань.

23.4. Навчання не може зводитися лише до підписання документа про ознайомлення та має містити практичні приклади, аналіз ризиків і способи перевірки результатів.

23.5. Координаційна група у взаємодії з відділом моніторингу якості освіти щорічно збирає узагальнену інформацію про офіційно впроваджені системи, використання в освітньому процесі, навчання, інциденти, звернення та потребу в оновленні правил.

23.6. Моніторинг не передбачає тотального спостереження за особистими обліковими записами, змістом приватних запитів або іншої надмірної обробки даних.

23.7. Щорічний узагальнений звіт містить оцінку користі і ризиків, стан реєстру систем, результати навчання, типові проблеми, інциденти у знеособленій формі та пропозиції щодо вдосконалення.

23.8. Звіт подається ректору та враховується у загальному звіті про функціонування системи забезпечення академічної доброчесності і внутрішньої системи забезпечення якості освіти.

23.9. Політика та методичні матеріали переглядаються з урахуванням законодавства, технологічних змін, практики застосування, результатів моніторингу та позицій академічної спільноти.

23.10. Університет може проводити пілотні проєкти за умови обмеженого масштабу, добровільності участі, мінімізації даних, визначених критеріїв успішності, можливості припинення та попереднього інформування учасників.

24. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

24.1. Ця Політика схвалюється Вченою радою Університету, вводиться в дію наказом ректора та набирає чинності з дня, визначеного відповідним наказом.

24.2. Політика оприлюднюється на офіційному вебсайті Університету та доводиться до відома заінтересованих осіб через офіційні канали комунікації.

24.3. Зміни та доповнення до Політики вносяться у порядку, установленому для її прийняття.

24.4. Політика переглядається в разі зміни законодавства, істотних технологічних змін або виявлення нових ризиків, а також за результатами моніторингу, але не рідше ніж один раз на три роки.

24.5. Питання, не врегульовані Політикою, вирішуються відповідно до законодавства України, Статуту Університету та інших локальних нормативних актів.

24.6. У разі прийняття нормативно-правового акта, який установлює інші або додаткові вимоги до використання технологій штучного інтелекту, застосовується такий акт, а Політика підлягає невідкладному приведенню у відповідність.

Розробник:

Проректор з науково-педагогічної роботи  Михайло МАЛЬОВАНИЙ

Погоджено:

Голова Первинної профспілкової організації Уманського національного університету _____ Маргарита ПАРУБОК

Голова Профспілки працівників, студентів, аспірантів та докторантів Уманського національного університету _____ Леся КАРНАУХ

Голова ради студентського самоврядування Уманського національного університету _____ Вікторія ГУРСЬКА

Голова Наукового товариства студентів, аспірантів, докторантів та молодих учених _____ Юлія УЛЯНИЧ

Додаток А

МАТРИЦЯ РІВНІВ РИЗИКУ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Рівень	Типові приклади	Основні умови	Порядок схвалення
1. Мінімальний	Перевірка правопису; технічне форматування; транскрибування власного мовлення; перетворення формату; засоби доступності; пошук ключових слів.	Не змінює змістовий результат; не використовує захищені дані; результат перевіряється користувачем.	Індивідуальне використання без окремого погодження; офіційна інтеграція оцінюється технічним підрозділом.
2. Обмежений	Генерування чернетки, структури, зображення, коду; переклад; узагальнення; аналіз даних; підготовка навчальних матеріалів; чернетка зворотного зв'язку.	Декларування суттєвого використання; перевірка фактів, джерел і прав; відсутність рішення істотного впливу; дані – лише дозволених категорій.	Для індивідуального використання – дотримання Політики; для офіційної закупівлі чи інтеграції – попереднє оцінювання.
3. Високий	Вступ, оцінювання, атестація, стипендії, мобільність, прогноз відрахування, кадровий добір, дисциплінарні процедури, біометрія, профілювання, значні масиви чутливих даних.	Документоване оцінювання впливу; правова і безпекова експертиза; людський контроль; повідомлення особи; журналювання; можливість оскарження; періодичний перегляд.	Рішення ректора або уповноваженої особи на підставі рекомендації Координаційної групи.
4. Заборонене використання	Повністю автоматизоване остаточне рішення; соціальне рейтингування; приховане маніпулювання; неправомірне розпізнавання емоцій; фабрикація даних; обхід безпеки; несанкціоноване введення захищеної інформації; немарковані оманливі deepfake-матеріали.	Не допускається незалежно від очікуваної користі, крім прямо встановленого законом винятку.	Не схвалюється. Виявлене використання припиняється та за потреби передається на розгляд за відповідною процедурою.

Примітка. Рівень ризику визначається не лише назвою системи, а конкретною метою, категоріями даних, масштабом, ступенем людського контролю та можливими наслідками використання.

Додаток Б

РЕЖИМИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У НАВЧАЛЬНИХ ЗАВДАННЯХ

Режим	**Що дозволено**	**Що заборонено**	**Орієнтовне формулювання для завдання**
1. Використання заборонене	Суто технічні засоби та засоби доступності, які не створюють змістовної відповіді, якщо викладач не встановив суворішої вимоги.	Генерування тексту, розв’язку, коду, висновків, зображень або іншого змістовного результату; перефразування готової відповіді; одержання підказок по суті завдання.	«Завдання виконується без використання генеративного штучного інтелекту. Дозволені лише засоби перевірки правопису та доступності, що не змінюють зміст роботи».
2. Обмежене використання	Лише функції, прямо визначені викладачем: пошук ідей, план, мовне редагування, переклад, пояснення поняття, допомога з кодом, візуалізація або інше.	Вихід за межі дозволених функцій; подання згенерованого змісту як повністю власного; приховування суттєвого використання; використання неперевірених джерел.	«Дозволено використати ШІ для _____. У декларації необхідно зазначити систему, мету та спосіб перевірки результату. Остаточний текст і висновки створює та обґрунтовує здобувач».
3. Використання дозволене або передбачене	Використання системи як об’єкта дослідження або повноцінного інструменту для генерування, порівняння, критики, моделювання чи створення прототипу відповідно до мети завдання.	Неперевірене копіювання; вигадані факти, джерела або дані; порушення прав третіх осіб; завантаження заборонених даних; відсутність особистого аналізу.	«Використання ШІ є частиною завдання. Оцінюються постановка запитів, критична перевірка, обґрунтоване доопрацювання результату, дотримання правил цитування та повна декларація використання».

Примітка. Викладач може деталізувати режим з урахуванням результатів навчання, форми контролю, доступності інструментів та вимог освітнього компонента, але правила мають бути доведені до здобувачів до початку виконання завдання.

Додаток В

ДЕКЛАРАЦІЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Автор (прізвище, ім’я, по батькові) _____

Назва роботи / завдання _____

Освітній компонент / проєкт / вид діяльності _____

Назва системи, постачальник, версія (за наявності), дата використання _____

Мета використання _____

Етапи роботи та характер допомоги системи _____

Орієнтовний обсяг матеріалу, згенерованого або опрацьованого системою _____

Спосіб перевірки фактів, джерел, обчислень, коду та інших результатів _____

Відомості про промпти, журнали або місце їх зберігання, якщо це вимагається _____

Підтверджую, що зазначив(ла) всі істотні способи використання технологій штучного інтелекту, особисто перевірив(ла) отримані результати, не включав(ла) вигаданих джерел або даних та несу відповідальність за остаточний зміст роботи.

Дата _____

Підпис _____

Додаток Г

ФОРМА ПОПЕРЕДНЬОГО ОЦІНЮВАННЯ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Ініціатор / структурний підрозділ _____

Назва системи та постачальник _____

Мета впровадження і очікувана користь _____

Категорії користувачів _____

Категорії даних, що вводяться або створюються _____

Результати системи та рішення, на які вони можуть впливати _____

Спосіб інтеграції з інформаційними ресурсами Університету _____

Можливий вплив на права, освіту, працевлаштування або доступ до можливостей _____

Відомі обмеження, ризики помилок, упереджень і безпеки _____

Механізм людського контролю та перегляду результату _____

Ліцензійні умови, вартість і строк використання _____

Запропонований пілотний період і критерії успішності _____

Висновок Координаційної групи:

Визначений рівень ризику _____

Умови та обмеження використання _____

Необхідні правова, технічна, безпекова, етична або інша експертиза _____

Рекомендація щодо пілотування, схвалення, доопрацювання або відмови _____

Дата _____

Підписи _____

Додаток Ґ

ПАСПОРТ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Назва системи	
Постачальник / правовласник	
Відповідальний підрозділ і відповідальна особа	
Мета та дозволені сценарії використання	
Рівень ризику	
Категорії користувачів	
Дозволені категорії даних	
Заборонені категорії даних	
Правова підстава обробки даних	
Місце та строки зберігання	
Використання постачальником введених даних для навчання моделі	
Відомі обмеження і ризики	
Механізми людського контролю	
Повідомлення та інструкції для користувачів	
Можливість оскарження або перегляду результату	
Кібербезпека та управління доступом	
Документ і дата схвалення	
Дата наступного перегляду	
Порядок припинення використання та видалення даних	

Додаток Д

ПОВІДОМЛЕННЯ ПРО ІНЦИДЕНТ, ПОВ’ЯЗАНИЙ ІЗ ВИКОРИСТАННЯМ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Заявник та контактні дані _____

Дата і приблизний час інциденту _____

Назва системи _____

Структурний підрозділ / вид діяльності _____

Опис події _____

Категорії даних або осіб, яких стосується інцидент _____

Відомі або можливі наслідки _____

Невідкладні дії, уже вжиті заявником чи підрозділом _____

Додатки та докази _____

Дата _____

Підпис _____

Примітка. Про витік персональних даних, несанкціонований доступ, виконання небезпечного коду або інший кіберінцидент необхідно повідомити невідкладно через офіційний канал Університету, не очікуючи заповнення повної форми.

Додаток Е

ПРИКЛАДИ ВІДПОВІДАЛЬНОГО, НЕНАЛЕЖНОГО ТА ЗАБОРОНЕНОГО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Сфера	**Відповідальне використання**	**Неналежне або заборонене використання**	**Декларування / контроль**
Навчальна робота	Пошук ідей, пояснення складного поняття, мовне редагування або аналіз прикладу в межах режиму, визначеного викладачем; самостійна перевірка та доопрацювання.	Подання згенерованої відповіді як власної; використання ШІ, коли воно заборонене; приховування істотного використання; вигадані джерела.	Режим установлюється до виконання завдання; суттєве використання декларується; за потреби подаються чернетки або промпти.
Кваліфікаційна робота	Допомога з планом, мовою, кодом, візуалізацією чи аналізом за умови дозволу, перевірки та опису методики.	Генерування основного дослідницького результату без особистого внеску; вигадані дані; недекларований згенерований текст; підміна авторства.	Декларація автора; опис у методології або примітці; збереження матеріалів, необхідних для перевірки відтворюваності.
Оцінювання	Створення чернетки тестових завдань, рубрики або зворотного зв’язку з обов’язковою перевіркою викладачем.	Остаточна оцінка виключно системою; таємне профілювання; санкція лише за показником детектора; дискримінаційний алгоритм.	Здобувача інформують про істотне застосування; остаточне рішення приймає людина; забезпечується пояснення та оскарження.
Наукове дослідження	Допомога з кодом, аналізом, перекладом, оглядом підходів або візуалізацією з перевіркою, документуванням і дотриманням протоколу.	Фабрикація спостережень, респондентів або результатів; вигадані посилання; приховане перетворення даних; введення конфіденційних даних без підстави.	Опис системи, версії, мети та істотних параметрів; збереження промптів і журналів, якщо це потрібно для відтворюваності.
Рецензування та експертиза	Допоміжна перевірка мови або структури без розкриття матеріалу і без підміни професійного судження, якщо це дозволено процедурою.	Завантаження неопублікованого рукопису до відкритого сервісу; автоматичне формування висновку без перевірки; розкриття особи автора.	Суттєве використання зазначається у висновку; конфіденційність і особиста відповідальність експерта зберігаються.

Сфера	Відповідальне використання	Неналежне або заборонене використання	Декларування / контроль
Адміністративна діяльність	Чернетка листа, переклад, класифікація звернень або узагальнення загальнодоступних даних із перевіркою посадовою особою.	Автоматичне видання наказу; неперевірена юридична чи фінансова інформація; завантаження особових справ; рішення про працівника без людини.	Офіційний документ перевіряє і підписує уповноважена особа; система не набуває статусу автора чи посадової особи.
Публічна комунікація	Створення чернетки допису, ілюстрації або субтитрів із фактичною перевіркою, правомірним використанням зображень і редакційним контролем.	Немаркований оманливий deepfake; вигадана цитата керівника; підроблені фото подій; маніпулятивний персоналізований вплив.	Синтетичний матеріал маркується, якщо може бути сприйнятий як автентичний; за публікацію відповідає визначений працівник.
Персональні дані	Робота зі знеособленими або мінімізованими даними у схваленій системі з визначеною метою та контролем доступу.	Введення паспортних, медичних, кадрових, освітніх або біометричних даних до відкритого сервісу без правової підстави й оцінювання ризику.	Використовуються лише дозволені категорії даних; доступ журналюється; строки зберігання та видалення визначаються до початку обробки.