2. Зачек О. І. Проблеми злочинного застосування штучного інтелекту. 2025. С. 32–34. URL: https://surl.li/cynjgl (дата звернення: 25.09.2025).

3. Юхно О. Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні. *Теорія та практика судової експертизи і криміналістики.* 2021. С. 40–59.

4. Кириченко В. В. Вплив штучного інтелекту на злочинність в Україні. 2025. С. 30–32. URL: https://surl.li/gwvrbs (дата звернення: 25.09.2025).

5. Андрущенко О. П. Захист прав людини в умовах розвитку штучного інтелекту. *Наукові дослідження*. 2024. С. 186–193.

Насальська Анна Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВЛЕННІ ТА ПОПЕРЕДЖЕННІ КІБЕРЗЛОЧИНІВ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА

Штучний інтелект (ШІ) займає провідне місце у розвитку сучасних технологій, зокрема у сфері кібербезпеки. Збільшення обсягів цифрової інформації та ускладнення видів кіберзлочинів вимагають впровадження ефективних інструментів для їх виявлення та попередження. Завдяки своїй здатності аналізувати великі масиви даних, розпізнавати закономірності та прогнозувати потенційні загрози, ШІ відкриває нові горизонти у боротьбі з кіберзлочинністю.

Проте активне впровадження ШІ у цю сферу супроводжується низкою викликів, зокрема пов'язаних з правовим регулюванням його застосування. Кримінальне право, що традиційно орієнтується на людську діяльність та відповідальність, змушене адаптуватися до нових реалій, де рішення приймаються автоматизованими системами на базі алгоритмів. Це породжує складнощі у визначенні суб'єктів відповідальності, контролі за законністю дій ШІ та захисті прав осіб.

У доповіді буде детально проаналізовано сучасні підходи до використання штучного інтелекту у виявленні та попередженні кіберзлочинів, розглянуто перспективи розвитку таких систем, а також обґрунтовано необхідність оновлення кримінально-правових норм задля ефективної регуляції нових технологій при збереженні балансу між безпекою та захистом прав людини.

Кіберзлочинність є однією з найгостріших проблем сучасного інформаційного суспільства. Зі збільшенням обсягу цифрових даних і розвитку інтернету з'являються нові види загроз, які суттєво впливають на безпеку держави, бізнесу та громадян. Особливо актуальним це питання стало для України у зв'язку зі зростанням кількості кібератак та складністю їх виявлення та попередження. В таких умовах штучний інтелект (ШІ) набуває все більшого значення як інноваційний інструмент для боротьби з кіберзлочинністю. Водночас застосування ШІ у цій сфері ставить низку правових, етичних і технологічних викликів, що потребують комплексного аналізу в рамках кримінального права.

Метою цієї доповіді є всебічне дослідження застосування ШІ для виявлення та попередження кіберзлочинів в Україні, аналіз переваг та обмежень цієї технології, а також розгляд викликів, пов'язаних із нормативно-правовим регулюванням її використання.

За останні роки кіберзлочинність в Україні значно зросла. У 2024 році було зареєстровано понад 4 300 кіберінцидентів, що на 70 % більше, ніж у 2023 році. Найновіші кіберзлочини охоплюють фішингові атаки, розповсюдження шкідливого програмного забезпечення, кібершпигунство, а також кібертероризм, часто синхронізований з фізичними атаками на критичну інфраструктуру країни.

Особливої уваги заслуговує зростання масштабних кібернападів на державні та оборонні об'єкти, у тому числі місцеві органи влади і ключові підприємства. Більшість українських організацій, за даними досліджень, все ще не має достатнього рівня кіберзахисту – близько 70 % компаній у 2024 році не інвестували в необхідні системи безпеки.

На державному рівні Україна активізувала роботу з удосконалення законодавства в цій сфері. У березні 2025 року Верховна Рада ухвалила закон «Про кіберзахист державних інформаційних ресурсів та об'єктів критичної інфраструктури», а в квітні 2025 року його підписав Президент України. Закон передбачає створення національної системи реагування на кіберінциденти, включаючи CERT-UA і галузеві команди реагування.

У боротьбі з кіберзлочинами ШІ застосовується передусім через алгоритми машинного навчання і глибинного навчання для визначення аномалій у мережевому трафіку, автоматичного розпізнавання образів і поведінкових патернів користувачів. Особливу роль відіграють системи прогнозування кібератак на базі історичних даних та автоматизованого аналізу великих обсягів інформації. Також ШІ допомагає оптимізувати роботу правоохоронців: від автоматичного контролю за порушеннями до виявлення потенційно небезпечних осіб за допомогою соціальних мереж і відеоспостереження.

В Україні офіційно використовується програмне забезпечення з елементами ШІ, зокрема «Касандра», яка дає можливість аналізувати й прогнозувати повторні порушення закону злочинцями, а також розгортаються аеророзвідки з використанням безпілотників для різного роду моніторингових і захисних функцій.

Впровадження ШІ у правоохоронні органи України значно підвищує ефективність виявлення кіберзагроз та оперативність реагування. Кіберполіція, Служба безпеки України (СБУ) активно співпрацюють із приватним сектором і ІТ-компаніями для впровадження сучасних рішень захисту. Застосування ШІ також допомагає підвищити професійний рівень кадрів завдяки сучасним навчальним системам і тренінгам.

Крім того, автоматизація рутинних операцій та прогнозування загроз дозволяє краще планувати ресурси і запобігати потенційним атакам на ранніх етапах. Незважаючи на

значні переваги, використання ШІ у правоохоронній діяльності не позбавлене викликів. Зокрема, виникають питання юридичної відповідальності у разі помилкових рішень автоматизованих систем, а також складність визначення винності в умовах використання ШІ при розслідуванні. Проблематичним є і захист прав людини: конфіденційність персональних даних, можливість дискримінації через упереджені алгоритми, а також довіра суспільства до рішень, прийнятих машинами.

Важливою є і правова невизначеність у сфері використання ШІ, що потребує спеціального законодавчого врегулювання із захистом громадянських свобод і встановленням чітких процедур контролю за застосуванням таких технологій. Досвід ЄС, США та інших країн показує, що успішне застосування ШІ у кримінальному праві можливе за умови чіткого правового регулювання, прозорості алгоритмів і контролю за процесом їх використання. Важливими є етичні стандарти, які мають базуватися на повазі до прав людини, та багатостороннє співробітництво для обміну знаннями і швидкого реагування на глобальні кіберзагрози.

Для України критично необхідно адаптувати законодавство відповідно до міжнародних стандартів і створити мультидисциплінарні команди експертів із технологій, права та етики.

Штучний інтелект – ключовий інструмент для ефективної боротьби з кіберзлочинністю в Україні, що дозволяє швидко і точно виявляти загрози та запобігати злочинам. Водночас його впровадження вимагає вдосконалення законодавчої бази, балансування між безпекою і правами громадян, а також постійного розвитку професійних кадрів. Використання ШІ в кримінальному праві повинно базуватися на етичних принципах і прозорості, що дозволить відбудувати довіру суспільства до нових технологій і зміцнити кібербезпеку держави.

Список використаних джерел

1. Верховна Рада України. Закон України «Про кіберзахист державних інформаційних ресурсів та об’єктів критичної інфраструктури». 2025 р.

2. Президент України. Офіційне повідомлення про підписання закону про кіберзахист державних ресурсів. 2025.

3. Forbes Україна. В Україні за рік кількість кібератак зросла на 70%. 27 вересня 2025 року.

4. Synchron.ua. Кібератаки на бізнес України 2025: Нові Вектори Загроз та Виклики. 2025.

5. Detector Media. Верховна Рада ухвалила закон про кіберзахист державних ресурсів. 2025.

6. LSEJ (Legal Studies and Economic Journal). Роль технологій штучного інтелекту у правоохоронній діяльності. 2024.

7. BDO Україна. Роль штучного інтелекту в кібербезпеці: передбачення і запобігання атак. 2025.

8. Visnyk Juris (Журнал юридичних досліджень). Зарубіжний досвід використання штучного інтелекту для протидії кіберзлочинам. 2025.

9. LIGA360. Державне регулювання штучного інтелекту в Україні. 2025.

10. НАВС (Національна академія внутрішніх справ України). Міжнародний досвід правового регулювання небезпеки ШІ. 2025.

11. Держателеві дослідження та аналітика українського ринку кібербезпеки 2017-2025 років, MS Detector.

Радіонова Валерія Іванівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРБУЛІНГ І ПЕРЕСЛІДУВАННЯ В МЕРЕЖІ: ПРОГАЛИНИ ЗАКОНОДАВСТВА

У цифрову епоху Інтернет перетворився не лише на зручний засіб спілкування, але й на простір, де все частіше фіксуються випадки психологічного насильства, зокрема