– публічно-приватна платформа обміну даними;

– законодавче оновлення стандартів.

Висновки. ШІ змінює правила гри у кіберпросторі: атаки стають більш масштабними, персоналізованими й дешевими. Україна має створити комплексну політику, яка поєднує технічні рішення, кадрову підготовку, нормативну базу та етичні стандарти. Круглий стіл може стати платформою для вироблення дорожньої карти впровадження таких змін.

Список використаних джерел:

1. CERT-UA – Офіційний сайт Національної команди реагування на кіберінциденти. https://cert.gov.ua/

2. РНБО України. Річний аналітичний огляд кіберзагроз, 2024–2025.

3. Vavryk Y., Opirskyy I. Штучний інтелект: кібербезпека нового покоління. Ukrainian Scientific Journal of Information Security, 2024.

4. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні, 2024.

5. Аналітичні матеріали Київстар Hub – «Тренди кібербезпеки на 2025 рік».

Гусол Олексій Дмитрович
Студент н.гр. 104_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

СУЧАСНІ ВИКЛИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

У сучасному світі інформаційні технології стали невід’ємною частиною економіки, політики, освіти та безпеки. Водночас активна цифровізація створює передумови для виникнення нових загроз у сфері кібербезпеки. Під кібербезпекою розуміють стан захищеності кіберпростору, при якому забезпечується цілісність, конфіденційність і доступність інформації. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», держава зобов’язана створювати систему захисту критичної інфраструктури та інформаційних ресурсів від кібератак. Одним із головних викликів сьогодення є зростання кількості цілеспрямованих атак на державні установи та правоохоронні органи.

Використання штучного інтелекту у злочинних цілях – це нова тенденція, яка ускладнює виявлення та запобігання кіберзлочинам. Атаки стають дедалі складнішими: кіберзлочинці використовують фішингові кампанії, шкідливе програмне забезпечення, методи соціальної інженерії. Особливої уваги потребує захист персональних даних громадян та державних реєстрів, оскільки їх витік може мати масштабні наслідки.

Важливу роль у протидії кіберзагрозам відіграє міжнародне співробітництво. Україна є учасником Будапештської конвенції про кіберзлочинність, що встановлює стандарти міжнародного обміну інформацією та спільного реагування на кібератаки. Крім того, розвиток кіберосвіти та підготовка кваліфікованих фахівців у сфері безпеки мають стати стратегічним напрямом державної політики.

Отже, сучасні виклики у сфері кібербезпеки вимагають системного підходу — поєднання технологічних, правових та освітніх заходів, спрямованих на захист державних і приватних ресурсів у кіберпросторі.

Розвиток сучасних технологій докорінно змінює функціонування правової системи, роботу правоохоронних органів і навіть психологічні підходи до вивчення поведінки людини. Використання штучного інтелекту, великих даних, відеоаналітики та цифрових платформ дозволяє підвищити ефективність правозастосовної діяльності, проте породжує нові правові та етичні дилеми.

У сфері права технології забезпечують автоматизацію процесів, зокрема електронне судочинство, електронні докази та використання блокчейн-систем для зберігання юридично значущих даних. Проте надмірна цифровізація створює ризики для конфіденційності особистої інформації. Використання алгоритмів прийняття рішень може призводити до помилкових або упереджених висновків, що ставить під сумнів принцип справедливості.

Правоохоронна діяльність сьогодні активно інтегрує технології відеоспостереження, біометрії та штучного інтелекту. Це сприяє ефективнішому розслідуванню злочинів, однак водночас вимагає чіткого правового регулювання збору, зберігання та використання персональних даних. Українське законодавство поступово адаптується до цих змін, спираючись на положення Закону «Про захист персональних даних» та міжнародні стандарти, такі як Загальний регламент ЄС із захисту даних (GDPR).

У психологічній практиці технології використовуються для аналізу емоційного стану, прогнозування поведінки та оцінки психічного здоров’я. Проте постає питання етичності таких методів, адже втручання в психіку людини через алгоритми або нейромережі може порушувати її право на приватність та самовираження.

Отже, впровадження сучасних технологій у право, правоохоронну діяльність і психологію потребує комплексного балансу між ефективністю, етикою та захистом прав людини. Це ключова умова розвитку безпечного цифрового суспільства в Україні.