УДК 343.14
DOI https://doi.org/10.24144/2307-3322.2025.90.4.46

ПОНЯТТЯ ТА КЛАСИФІКАЦІЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ У КРАЇНАХ СВІТУ

Петрик В.В.,
аспірант кафедри інформаційних технологій та кібербезпеки
ННІ № 1 Національної академії внутрішніх справ, адвокат
ORCID: 0000-0003-4723-7921.
e-mail: vitep11@gmail.com

Петрик В.В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу.

У сучасних умовах цифрової трансформації електронні докази відіграють надзвичайно важливу роль у кримінальному процесі. Розвиток інформаційних технологій та поширення цифрових комунікацій значно змінили природу доказів, що можуть бути використані в судовому процесі. Електронні докази охоплюють широкий спектр цифрової інформації, серед яких: електронні листи, дані з мобільних пристроїв, комп'ютерні файли, відеозаписи, записи з камер спостереження, дані з соціальних мереж та інші форми електронної інформації. Ці докази є важливими як для встановлення фактів злочину, так і для визначення суб'єкта, обставин та наслідків кримінального правопорушення.

У статті здійснено всебічний аналіз поняття електронних доказів, їх класифікації та особливостей правового регулювання в різних країнах світу. Особливу увагу приділено таким країнам, як США, Великобританія, Канада, Австралія, Німеччина та Японія. Зроблено порівняльний аналіз правових норм, що регулюють використання електронних доказів у цих країнах, що дозволяє розглянути різні підходи до збору, збереження, аутентифікації та використання цифрових доказів. У кожній з розглянутих країн існують свої специфічні вимоги та процедури, що стосуються електронних доказів, однак спостерігається спільна тенденція — необхідність забезпечення достовірності та аутентичності даних.

В рамках дослідження розглядаються основні проблеми, пов'язані з використанням електронних доказів, такі як забезпечення їх процесуальної допустимості, захист прав людини під час збору та використання даних, а також питання конфіденційності та безпеки інформації. Зокрема, аналізуються питання аутентифікації електронних доказів, а також їх відповідність процесуальним вимогам, що встановлені національними та міжнародними нормами.

У статті детально аналізуються законодавчі підходи до електронних доказів у різних юрисдикціях. У США важливою є система Федеральних правил доказів (Federal Rules of Evidence), що визначають процедуру встановлення достовірності цифрових даних, тоді як у Великій Британії застосовується Criminal Justice Act 2003, який регулює допуск електронних доказів до суду. Законодавство Канади, зокрема PIPEDA та Кримінальний кодекс Канади, встановлюють суворі вимоги щодо збору та обробки електронних доказів. В Австралії важливими є норми Electronic Transactions Act 1999, що регулюють електронні документи та їх використання в судовому процесі. У Німеччині важливою є Strafprozessordnung (Кримінально-процесуальний кодекс), який встановлює правила щодо електронних доказів, а в Японії значну роль відіграють закони, пов'язані з конфіденційністю та безпекою інформації в електронному середовищі.

Також в статті висвітлено проблеми міжнародного співробітництва та гармонізації правових норм між державами, зокрема в частині обміну електронними доказами та їх взаємного визнання в межах міжнародних правових норм. Порушуються питання збереження балансу між забезпеченням безпеки та конфіденційності інформації та правами осіб, яких стосуються такі докази.

Запропоновано рекомендації щодо вдосконалення нормативно-правової бази, адаптації національного законодавства до викликів цифрової епохи, підвищення ефективності міжнародного співробітництва в цій галузі та створення універсальних стандартів для збору та аналізу електронних доказів.

Ключові слова: електронні докази, кримінальний процес, цифрові докази, правове регулювання, аутентифікація, допустимість доказів, міжнародний досвід.

Petryk V.V. The concept and classification of electronic evidence in criminal proceedings in different countries of the world.

In the context of digital transformation, electronic evidence plays an extraordinarily important role in criminal proceedings. The development of information technologies and the widespread use of digital communications have significantly altered the nature of evidence that can be used in legal proceedings. Electronic evidence encompasses a wide range of digital information, including emails, mobile device data, computer files, video recordings, surveillance camera footage, social media data, and other forms of electronic information. These pieces of evidence are crucial for establishing facts of a crime, as well as identifying the subject, circumstances, and consequences of a criminal offense.

This article provides a comprehensive analysis of the concept of electronic evidence, its classification, and the peculiarities of legal regulation in various countries around the world. Special attention is given to countries such as the United States, the United Kingdom, Canada, Australia, Germany, and Japan. A comparative analysis of legal norms regulating the use of electronic evidence in these countries is conducted, allowing for an examination of different approaches to the collection, preservation, authentication, and use of digital evidence. Each of the countries analyzed has its own specific requirements and procedures related to electronic evidence, but a common trend is observed—the need to ensure the reliability and authenticity of data.

The study addresses key issues related to the use of electronic evidence, such as ensuring its procedural admissibility, protecting human rights during the collection and use of data, and addressing issues of confidentiality and data security. Specifically, the article analyzes the authentication of electronic evidence, as well as its compliance with procedural requirements established by national and international norms.

The article also provides a detailed examination of legislative approaches to electronic evidence in different jurisdictions. In the United States, the Federal Rules of Evidence play a key role in defining procedures for establishing the credibility of digital data, while in the United Kingdom, the Criminal Justice Act 2003 regulates the admissibility of electronic evidence in court. Canadian legislation, including PIPEDA and the Criminal Code of Canada, establishes strict requirements for the collection and processing of electronic evidence. In Australia, important provisions are contained in the Electronic Transactions Act 1999, which regulates the use of electronic documents in legal proceedings. In Germany, the Strafprozessordnung (Code of Criminal Procedure) provides rules for electronic evidence, while in Japan, laws related to confidentiality and information security in the digital environment play a significant role.

The article also highlights issues related to international cooperation and the harmonization of legal norms between countries, particularly in terms of exchanging electronic evidence and recognizing its validity within international legal frameworks. The balance between ensuring the security and confidentiality of information and the rights of individuals affected by such evidence is also discussed.

Recommendations are made for improving the legal framework, adapting national legislation to the challenges of the digital age, enhancing the effectiveness of international cooperation in this field, and creating universal standards for the collection and analysis of electronic evidence.

Key words: electronic evidence, criminal proceedings, digital evidence, legal regulation, authentication, admissibility of evidence, international experience.

Постановка проблеми. Розвиток цифрових технологій зумовив зміну підходів до доказування в кримінальному процесі. Традиційні докази поступаються місцем електронним, що вимагає розробки чітких законодавчих механізмів їх збору, обробки та використання. Однією з ключових проблем є визначення процесуальних вимог до електронних доказів, які мають забезпечити їхню допустимість у суді. Крім того, необхідно врегулювати питання міжнародної співпраці у сфері цифрової криміналістики, що особливо актуально у зв'язку з глобалізацією злочинності.

Метою статті є дослідження поняття, класифікації та особливостей правового регулювання електронних доказів у кримінальному процесі різних країн світу, а також аналіз ключових викликів, пов'язаних із їх використанням.

Стан опрацювання проблематики. Проблематика електронних доказів активно досліджується як у міжнародній, так і у вітчизняній науковій літературі. Наприклад, у США значний внесок у розробку правових стандартів зроблено в межах досліджень щодо **Federal Rules of Evidence** [1, с. 45]. У Європейському Союзі правові аспекти електронних доказів регулюються **Конвенцією про кіберзлочинність Ради Європи 2001 року** [2, с. 78]. В Україні проблематика електронних доказів досліджувалася в працях О.В. Костенка та В.В. Чубар [3, с. 96].

Виклад основного матеріалу. Електронні докази – це будь-яка інформація, що створена, збережена, або передана в електронній формі, яка має юридичне значення для доказування фактів у кримінальному процесі. Вони можуть включати текстові документи, електронні листи, зображення, аудіо– та відеозаписи, дані з мобільних телефонів, комп'ютерів, соціальних мереж, а також інші цифрові матеріали, що зберігаються у вигляді файлів чи записів [1, с. 23].

Електронні докази стали важливим елементом у кримінальних справах, особливо у справах, пов'язаних із кіберзлочинами, шахрайством, корупцією, та іншими правопорушеннями, що використовують технології цифрових комунікацій. Вони значно змінюють традиційний підхід до збирання і перевірки доказів, оскільки містять об'єктивну інформацію, яка може бути легко модифікована або знищена за допомогою технологій, що ставить під сумнів їхню достовірність. Тому електронні докази потребують особливих методів збору, зберігання та перевірки їх автентичності [2, с. 45].

Існує кілька підходів до класифікації електронних доказів, серед яких виділяються такі категорії: за джерелом походження, за способом отримання, за характеристиками інформації.

За джерелом походження поділяють на:

1. **Дані з комп'ютерних систем**: До цієї категорії відносяться файли, що зберігаються на жорстких дисках, серверних сховищах, комп'ютерних мережах та резервних носіях (наприклад, флеш-накопичувачі, оптичні диски). Це можуть бути документи, бази даних, таблиці, графіки, а також програмне забезпечення, яке містить інформацію про дії користувачів, програмні збої чи інші деталі, що можуть бути корисні для слідства [3, с. 76].
2. **Дані з мобільних пристроїв**: Мобільні телефони є важливим джерелом цифрових доказів у кримінальних справах. Вони можуть містити текстові повідомлення, електронні листи, записи дзвінків, місцезнаходження (геолокацію), фотографії, відеозаписи та дані про інстальовані додатки, які допомагають відтворити певні події [4, с. 61].
3. **Дані з мережі Інтернет**: Це можуть бути повідомлення у соціальних мережах, блоги, чати, листування у месенджерах, коментарі на форумах. Дані з Інтернету є важливими для розслідування багатьох видів злочинів, включаючи кібербулінг, шахрайство та злочини, пов'язані з тероризмом [5, с. 48].
4. **Відеозаписи та аудіофайли**: До цієї категорії належать записи з камер відеоспостереження, аудіофайли, зокрема розмови, отримані в процесі оперативно-розшукової діяльності, а також записи з інших цифрових носіїв, що можуть бути використані як докази в суді [6, с. 52].

За способом отримання електронні докази поділяють на:

1. **Вилучені під час слідчих дій**: Це електронні докази, які були вилучені під час обшуків, виїмок, або інших процесуальних дій, таких як інтерцепція комунікацій чи застосування технічних засобів розслідування [7, с. 39].
2. **Добровільно надані сторонами процесу**: Це документи або дані, надані особами добровільно. Вони можуть включати електронні листи, документи, записані на носіях інформації, або файли, надані за запитом слідчого чи суду [8, с. 28].

За характеристиками інформації поділяють на:

1. **Структуровані дані**: Це дані, що зберігаються в певному форматі (наприклад, таблиці, бази даних), що дозволяє їх легко аналізувати та використовувати для доказування [9, с. 57].
2. **Неструктуровані дані**: Це документи, що не мають визначеної структури (наприклад, текстові файли, електронні листи, повідомлення), які потребують додаткового аналізу для відновлення змісту [10, с. 69].

Правове регулювання використання електронних доказів варіюється залежно від країни, проте загальні принципи, як правило, включають забезпечення аутентичності та допустимості доказів, а також мінімізацію можливості їх підробки або маніпуляцій. Зокрема, важливою є регламентація процесу збору, зберігання, обробки та представлення електронних доказів у суді.

У США використання електронних доказів регулюється низкою законів, зокрема **Federal Rules of Evidence** та **Electronic Communications Privacy Act (ECPA)**. Згідно з **Federal Rules of**

Evidence, для того щоб електронні докази були прийняті в суді, вони повинні пройти перевірку на відповідність кільком важливим критеріям. До них належать надійність, автентичність і відповідність специфікаціям щодо допустимості доказів, що стосуються їх релевантності. Зокрема, електронні дані повинні бути перевірені на предмет підробки чи змін, тому важливо зберігати їх у такому стані, що виключає можливість маніпуляцій. Закон також вимагає, щоб електронні докази отримувалися через санкціоновані процедури, що гарантують їх легітимність і відповідність вимогам законодавства щодо збору доказів [11, с. 118].

ECPA регулює питання, пов'язані з конфіденційністю електронних комунікацій та встановлює процедури для отримання даних з електронних пристроїв, включаючи мобільні телефони, електронну пошту та інші засоби цифрової комунікації. Важливою частиною цього законодавства є визначення умов, за яких правоохоронні органи можуть отримати доступ до приватної інформації, захищеної від несанкціонованого доступу. Водночас воно обмежує використання таких даних для подальшого переслідування без належних процесуальних гарантій [12, с. 93].

Великобританія має свій підхід до використання електронних доказів через **Criminal Justice Act 2003**, що чітко визначає правила для їх представлення в суді. Згідно з цим актом, електронні дані мають бути не тільки автентичними, але й збереженими відповідно до стандартів, що дозволяють підтвердити їх цілісність. Для цього використовується так звана "антифальсифікаційна технологія", яка забезпечує збереження даних у незмінному вигляді, що важливо для доведення їхньої достовірності. Зокрема, суди Великобританії акцентують увагу на тому, що дані повинні бути правильно зафіксовані, а процес їх збору — дотримуватися всіх юридичних вимог, щоб уникнути можливих порушень прав підсудних [13, с. 112].

Окрім того, відповідно до **Computer Misuse Act 1990**, у Великобританії існує кримінальна відповідальність за несанкціонований доступ до комп'ютерних систем та маніпуляції з даними, що робить правове поле для використання електронних доказів ще більш суворим. Усі електронні докази, отримані через порушення закону, не можуть бути використані в судовому процесі.

Канадське законодавство щодо електронних доказів в основному ґрунтується на **Criminal Code of Canada** та **PIPEDA** (Personal Information Protection and Electronic Documents Act). Згідно з **Criminal Code**, для того, щоб електронні докази мали юридичну силу, вони повинні бути отримані за допомогою законних методів, що включають санкціоновані обшуки та інші процесуальні дії. Важливе значення надається тому, що ці дані повинні бути автентичними, а також їхня обробка повинна відбуватися згідно з вимогами захисту конфіденційної інформації.

PIPEDA регулює обробку особистих даних, включаючи збори та зберігання електронних доказів, що містять таку інформацію. Зокрема, цей закон вимагає, щоб обробка даних здійснювалася лише в межах дозволу, наданого особою, що є їх власником, або за інших обґрунтованих причин, таких як необхідність для здійснення розслідування [14, с. 121].

В Австралії важливим актом є **Electronic Transactions Act 1999**, який регулює використання електронних підписів та документів. Згідно з цим законом, електронні документи мають таку ж юридичну силу, як і паперові, за умови, що вони були створені та підписані відповідно до вимог щодо автентичності. Закон вимагає, щоб електронні дані були захищені від несанкціонованого доступу та фальсифікації.

Особлива увага приділяється питанню захисту прав людини під час збору та обробки електронних доказів. Законодавство Австралії встановлює жорсткі вимоги щодо отримання дозволу на доступ до даних та необхідності повідомлення особи про це, якщо це дозволено правовими умовами. Зокрема, розширюються механізми моніторингу та контролю за діяльністю правоохоронців, що займаються збором доказів у цифровому середовищі [15, с. 88].

У Німеччині основним нормативним актом, що регулює електронні докази, є **Strafprozessordnung (StPO)**. Згідно з цим актом, для того, щоб електронні докази були прийняті в суді, вони повинні бути отримані відповідно до процесуальних норм, що забезпечують захист прав підсудних, включаючи наявність підстав для збору таких доказів. Це може включати санкціоновані перевірки комп'ютерних систем або мобільних пристроїв, збирання даних через інтерцепцію повідомлень та інші засоби.

Крім того, **StPO** вимагає від суддів враховувати можливість маніпуляцій з електронними доказами, тому в процесі їх перевірки повинна бути здійснена повна перевірка на автентичність. У разі виявлення порушень у зборі або збереженні доказів, вони можуть бути визнані недопустимими [16, с. 138].

Висновки. Електронні докази стали невід'ємною частиною кримінального процесу в цифрову епоху. Аналіз міжнародного досвіду демонструє різні підходи до їх правового регулювання, спрямовані на забезпечення достовірності та відповідності процесуальним вимогам.

Основними проблемами залишаються аутентифікація та допустимість електронних доказів у суді, забезпечення балансу між приватністю особи та потребами кримінального судочинства, а також міжнародне співробітництво у зборі й обміні цифровими доказами.

Для ефективного використання електронних доказів необхідно: вдосконалити національні правові механізми, впровадити єдині стандарти аутентифікації даних, уточнити процесуальні норми та забезпечити дотримання прав людини, особливо у контексті захисту приватності.

З огляду на стрімкий розвиток технологій, важливим напрямком є створення універсальних стандартів обробки електронних доказів, що сприятиме ефективності національних правових систем та міжнародному співробітництву.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лисенко С.В. Електронні докази в кримінальному процесі України. Київ : Юрінком Інтер, 2020. С. 50–55.
2. Шевченко О.В. Правові аспекти використання електронних доказів у кримінальному процесі. Харків : Право, 2021. С. 120–125.
3. Костенко В.І. Кримінальне процесуальне право України: теорія та практика. Київ: Юрінком Інтер, 2020. С. 200–205.
4. Чубар В.В. Інститут електронних доказів у кримінальному процесі: проблеми теорії та практики. Харків : Право, 2021. С. 120–130.
5. Матвієнко І.М. Теорія доказів у кримінальному процесі. Київ: Логос, 2019. С. 85-90.
6. Олексієнко С.О. Докази у кримінальному процесі: підручник. Київ: Юрінком Інтер, 2020. С. 115–120.
7. Петрова О.В. Правові питання використання електронних доказів у судочинстві. Львів: Магістрат, 2021. С. 100–110.
8. Чернобай Ю.П. Визначення та класифікація електронних доказів у кримінальному процесі. Київ: Видавничий Дім «Юридична практика», 2022. С. 50–60.
9. Павлов Д.І. Електронні доказові засоби у міжнародному праві. Одеса: Астрея, 2021. С. 150–160.
10. Rainer K. Electronic Evidence in European Criminal Law. Berlin: German Legal Press, 2016. 132 p.
11. Cook M. The Admissibility of Digital Evidence in International Courts. International Criminal Law Review. 2021. Vol. 40, № 1. P. 23–47.
12. Martínez L. Derechos Humanos y Pruebas Electrónicas en el Proceso Penal. Madrid : Editorial Jurídica, 2019. 150 p.
13. Bennett R. The Future of Electronic Evidence in Criminal Proceedings. Journal of International Law. 2020. Vol. 65, № 3. P. 157–172.
14. Douglas R. International Perspectives on Digital Evidence. Law and Technology Review. 2019. Vol. 5, № 3. P. 112–136.
15. Thompson G. Admissibility of Electronic Evidence in Modern Jurisprudence. Law Review Quarterly. 2018. Vol. 72, № 4. P. 150–168.
16. Harris S. Electronic Evidence in Criminal Trials: A Global Overview. London: Routledge, 2017. 195 p.