

Неня Олена Володимирівна,

начальник першого науково-дослідного відділу науково-дослідної лабораторії криміналістичної та спеціальної техніки ДНДІ МВС України, кандидат юридичних наук;

Березненко Наталія Михайлівна,

провідний науковий співробітник другого науково-дослідного відділу науково-дослідної лабораторії криміналістичної та спеціальної техніки ДНДІ МВС України, кандидат технічних наук;

Корнійко Станіслав Миколайович,

науковий співробітник першого науково-дослідного відділу науково-дослідної лабораторії криміналістичної та спеціальної техніки ДНДІ МВС України

ШЛЯХИ ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ У СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Євроінтеграційні процеси, що відбуваються зараз в Україні, зумовлюють необхідність ґрунтовного дослідження зарубіжного досвіду адміністративно-правового регулювання експертної діяльності у сфері комп'ютерних технологій. Результати цього дослідження дають можливість визначити перспективи вдосконалення вітчизняного законодавства та відповідних адміністративних процедур [1, с. 270; 2, с. 12].

За результатами аналізу досвіду країн пострадянського простору, держав-членів ЄС, США, Великої Британії тощо визначено, що для кожної з цих країн характерна власна специфіка адміністративно-правового регулювання експертної діяльності у сфері комп'ютерних технологій. Водночас спільним є те, що в зарубіжних країнах в ході адміністративно-правового регулювання статусу експертів та процесу експертної діяльності широко використовуються ліцензування та акредитація експертних установ, професійна сертифікація (підтвердження компетенції) експертів, стандартизація (визначення єдиних алгоритмів) експертних процедур, валідація експертних методик тощо. Поширеною є практика прийняття міжнародних стандартів з питань експертної діяльності, а також у сфері обігу комп'ютерних технологій.

В умовах глобалізації та стрімкого розвитку інформаційного суспільства адміністративно-правове регулювання створення, впровадження, використання й виведення з експлуатації комп'ютерних технологій (їх компонентів), зокрема, з використанням таких засобів, як сертифікація комп'ютерних технологій (як продукції),

стандартизація в галузі комп'ютерних технологій, оцінка відповідності (зокрема, в частині дотримання вимог щодо безпеки та безпечності комп'ютерних технологій) є одним з основних напрямів забезпечення інформаційно-технологічного суверенітету, а також необхідною передумовою для належної реалізації інших складових адміністративно-правового регулювання експертної діяльності у сфері комп'ютерних технологій. Комп'ютерні технології сьогодні є рушійною силою освіти й науки, в т. ч. використовуються в ході підвищення та підтвердження кваліфікації експертів, а також при здійсненні практично будь-яких експертиз, зокрема й експертиз комп'ютерних технологій.

27 червня 2019 року в ЄС набрав чинності новий Регламент 2019/881 «Про Агентство ЄС з кібербезпеки (ENISA) і сертифікацію з кібербезпеки інформаційних і комунікаційних технологій», більш відомий під назвою «Акт про кібербезпеку» (Cybersecurity Act), який посилює мандат Європейського агентства мереж та інформаційної безпеки (ENISA), встановлює рамки ЄС для сертифікації кібербезпеки продуктів, послуг і технологічних процесів інформатики та засобів зв'язку, підвищуючи безпеку онлайн-послуг і споживчих пристроїв [3]. Акт встановлює єдиний фреймворк сертифікації в сфері кібербезпеки для інформаційних і комунікаційних технологій (ІТ). Акт передбачає добровільну сертифікацію ІТ продуктів, послуг і процесів. Проте акти ЄС або держав-членів можуть визначати сфери, в яких сертифікація продуктів, послуг або процесів буде обов'язковою. Згодом Європейська Комісія має оцінити ефективність такого підходу і встановити обов'язковість сертифікації в певних сферах діяльності, але вже зараз зрозуміло, що незабаром сертифікація з кібербезпеки стане стандартом роботи в країнах ЄС [4].

Щодо України, то варто зазначити, що наразі «сертифікація комп'ютерів» стосується практично всіх обчислювальних машин, за винятком комплектуючих запчастин до них (коди УКТ ЗЕД засобів обчислювальної техніки: 8471; 8473; 8504 40; 9008 30 00 00). Сертифікація комп'ютерів була обов'язковою процедурою згідно з Переліком продукції, що підлягає обов'язковій сертифікації в Україні, затвердженого Наказом Держспоживстандарту України від 01.02.2005 №28. З 01.01.2018 Україна повністю перейшла до процедур підтвердження відповідності сертифікації продукції та послуг за Європейськими принципами, тож сертифікація проводиться на підставі результатів випробувань, які за своїм змістом фактично становлять експертні дослідження [5].

Крім того, у всьому світі, зокрема і в Україні, стрімко оцифровуються фінансові послуги та сфера внутрішньої безпеки (документи, що засвідчують особу, інформація з системи моніторингу та збору інформації, електронні запити у кримінальних справах тощо). Все це не тільки актуалізує проблему захисту персональних даних, а й уможлиблює використання комп'ютерних технологій в організації

фінансових розкрадань, масових заворушень, терористичних актів, а також в управлінні збройними конфліктами. Активне використання зловмисниками методів соціальної інженерії та вразливостей, пов'язаних з використанням «Інтернету речей» [6], головна небезпека якого полягає в тому, що ІТ-системи створюють нові точки доступу для зловмисників, які оперують у кіберпросторі, – хакерів, кракерів тощо. При цьому, як пересічні громадяни, так і оператори об'єктів критичної інфраструктури й державні органи користуються іноземними операційними системами та антивірусними продуктами, що не сприяє забезпеченню кібербезпеки. У країні також використовується імпортне мережеве обладнання, яке може обслуговуватись зарубіжними розробниками дистанційно, а відтак в «потрібний» момент може бути виведено з ладу [7]. Саме тому суспільство сьогодні потребує надійних гарантій її стійкості до кібератак та інших критичних ситуацій, незалежно від того, чи спрямовані такі атаки проти державних органів, комерційних підприємств або фізичних осіб. Однією з таких гарантій, як бачимо, виступає сертифікація комп'ютерних технологій.

Проте сама сертифікація ІТ-продукту, послуги або процесу виступає результатом їх дослідження й оцінки за допомогою спеціальних знань, тобто експертного дослідження. Експертна діяльність у сфері комп'ютерних технологій, аби забезпечити належний рівень дослідження, зокрема, на предмет відповідності вимогам кібербезпеки, вимогам наукової і технологічної новизни, а також на предмет вирішення завдань кримінального судочинства, підлягає адміністративно-правовому регулюванню, зокрема, за допомогою таких інструментів, як стандартизація, сертифікація, акредитація та валідація. В усіх випадках рівень державної ваги робіт із сертифікації комп'ютерних технологій, і так само адміністративного регулювання експертної діяльності у сфері комп'ютерних технологій пропорційний рівню залежності країни від технологій зарубіжного виробництва і розвитку нових методів інформаційного протиборства, комп'ютерної злочинності тощо, адже саме реалії сучасного світу – розвиток комп'ютерних технологій та необхідність забезпечення кібербезпеки – зумовлюють необхідність виокремлення експертної діяльності у сфері комп'ютерних технологій як самостійного предмета дослідження й адміністративно-правового регулювання, незалежно від того, мова йде про судові або ж про несудові експертизи комп'ютерних технологій.

Міжнародний досвід в процесах організації та здійснення експертної діяльності показує, що існування вимог до акредитації та, відповідно, їхня реалізація сприяють розвитку методичного забезпечення завдяки диференціації проведених досліджень, з одного боку, а з іншого – ефективно сприяють кооперації при виконанні складних багато об'єктних експертиз, відкривають можливість інформаційного методичного обміну.

Не викликає заперечень й те, що сертифікація та валідація методичного забезпечення дадуть змогу з високою якістю вирішувати теоретичні та практичні завдання. При цьому мінімізуються можливі експертні помилки, підвищується ефективність використовуваних засобів і методів, знижуються матеріальні і тимчасові витрати на проведення досліджень і експертиз. Перспектива використання сертифікованих експертних методик, однотипні вимоги до експертів відповідних спеціальностей відкривають можливості досягнення порівнянних результатів при дослідженні тих самих об'єктів, а значить, підвищують об'єктивність і результативність проведених експертиз.

Список використаних джерел

1. Олійник О. О. Зарубіжний досвід адміністративно-правового регулювання судово-експертної діяльності. Митна справа. 2013. № 4 (88). С. 270-275.
2. Філоненко Р. Демократизація українського суспільства – засаднича складова входження України до простору Європи. Віче. 2011. № 2. С. 9-12.
3. ЕС создает сертификацию кибербезопасности информатики и связи. URL: <https://interfax.com.ua/news/telecom/510789.html>.
4. В ЕС договорились по закону о кибербезопасности. URL: <https://day.kyiv.ua/ru/news/111218-v-es-dogovorilis-po-kiberbezopasnosti>.
5. Про технічні регламенти та оцінку відповідності: Закон України від 15.01.2015. № 124-VIII. URL: <https://zakon.rada.gov.ua/laws/main/124-19#Text>.
6. Ревенков П.В. Финансовый мониторинг в условиях интернет-платежей. Москва. 2016. 64 с.
7. Ревенков П.В., Бердюгин А. А. ДБО: Интернет создает новых клиентов и расширяет профили рисков. Банковское дело. 2013. № 12. С. 64–67.

Нестор Наталія Володимирівна,

заступник директора з наукової роботи
Київського науково-дослідного інституту
судових експертиз Міністерства юстиції
України, доктор юридичних наук

СУДОВА ЕКСПЕРТИЗА: МИНУЛЕ, ТЕПЕРІШНЄ, МАЙБУТНЄ

Хто не пам'ятає свого минулого, той
не вартий свого майбутнього.

Максим Рильський

Становлення судової експертизи має тривалу історію, пов'язану з розвитком людської цивілізації, суспільних відносин, держави і права. Цю історію складають дати, події, люди, ідеї, досягнення і відкриття у різних галузях знань. На жаль, обсяг тез дозволяє навести лише декілька моментів з минулого судової експертизи.