Список використаних джерел:

1. Конституція України. URL : https://zakon.rada.gov.ua/laws/card/254%D0%BA/96-%D0%B2%D1%80.
2. Міжнародний пакт про економічні, соціальні і культурні права від 16.12.1966 р. URL : http://zakon2.rada.gov.ua/laws/show/995_042.
3. Національна стратегія у сфері прав людини: Указ Президента України від 24.03.2021 р. № 119/2021. URL: https://zakon.rada.gov.ua/laws/show/119/2021#Text.
4. Постанова Великої Палати Верховного Суду від 10.11.2022 р. у справі № 990/115/22. URL : http://iplex.com.ua/doc.php?regnum=107354803&red=100003a65502f2d8e1a89dbdb3e2e75aa1939e&d=5.
5. Про внесення змін до деяких законодавчих актів України щодо уточнення повноважень суб'єктів забезпечення цивільного захисту та імплементації норм міжнародного гуманітарного права у сфері цивільного захисту. Закон України від 09.07.2022 р. № 2394-IX. URL : https://zakon.rada.gov.ua/laws/show/2394-20#Text.
6. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII. URL : https://zakon.rada.gov.ua/laws/show/389-19#Text.
7. Славна О. В. Забзепечення прав і свобод людини в умовах правового режиму воєнного стану в Україні в контексті Національної стратегії у сфері прав людини. *Електронне наукове видання «Аналітично-порівняльне правознавство».* С. 45-49. URL : http://journal-app.uzhnu.edu.ua/article/view/264465/260635.

ВИГАНЯЙЛО Світлана Миколаївна,
доцент кафедри
соціально-економічних дисциплін
Сумської філії
Харківського національного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЕЛЕКТРОННІ ЦИФРОВІ ДОКАЗИ В УМОВАХ ВОЄННОГО СТАНУ

В умовах війни в Україні актуальним стає питання електронних цифрових доказів, як воєнних так і цивільних злочинів. Дуже багато питань постає з цього приводу, а саме: що ми можемо вважати електронним цифровим доказом (які формати можуть сприйматись у суді як докази, що є оригіналом, чи дублікатом, чи копією), хто та яким чином може збирати такі докази, яким чином і куди передавати.

В умовах збройної агресії рф в Україні надзвичайно актуальним є збір і документація воєнних злочинів, втім як і цивільних також. Розвиток науки і техніки, масове використання інформаційних технологій дозволяють збирати цифрові докази у вигляді, фото-, відео-, аудіо- файлів, електронні документи, дані з відкритих джерел, соціальних мереж. Спробуємо розібратись чи зможе ця інформація стати доказовою базою, та допомогти засудити воєнні злочини і злочини проти людяності?

Звернемось до Основних положень державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набув чинності з 1 січня 2019 року.

Стандарт ISO/IEC 27037:2012 надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів, такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть буті корисними на стадії аналізування потенційних цифрових доказів.

Цей стандарт також спрямовано на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для поліцейських підрозділів, які формують та запроваджують процедури щодо цифрових доказів, часто як частину доказів більшого об’єму.

Потенційні цифрові докази, розглянуті в цьому стандарті, можуть мати походження з різних типів цифрових пристроїв, мереж, баз даних тощо. Вони стосуються даних, які вже є в цифровому форматі. Цей стандарт не намагається охопити перетворення аналогових даних у цифровий формат.

Завдяки недовговічності цифрових доказів потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних цифрових доказів. Цей стандарт не вимагає обов’язкового використання винятковий інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією. Цей стандарт не стосується методології для законодавчих та дисциплінарних судових процесів, а також інших пов’язаних діяльностей під час оброблення потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження.

Запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Він не повинен заміняти специфічні законодавчі вимоги будь-якої юрисдикції. Фактично, він може слугувати практичною настановою для DEFR або DES у дослідженнях, які охоплюють потенційні цифрові докази. Він не впливає на аналізування цифрових доказів та не замінює специфічних юридичних вимог, що стосуються таких питань, як визнання доказів, доказова вага, значущість та інші юридично контрольовані обмеження використання потенційних цифрових доказів у судах. Цей стандарт може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями. Для підтримання цілісності цифрових доказів користувачам цього стандарту потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних законодавчих вимог юрисдикції для доказів.

Хоча цей стандарт не охоплює судової готовності, відповідна судова готовність може бути значною мірою підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність – це досягнення відповідного рівня здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізування цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, використовуваними в розслідуваннях інциденту після того, як він вже трапився, судова готовність є проєктивним процесом спроби планування процесу дослідження інциденту.

Цей стандарт відповідає ISO/IEC 27001 та ISO/IEC 27002, зокрема вимогам заходів щодо безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. Крім того, цей стандарт має застосування в контексті, незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт потрібно розглядати разом з іншими стандартами, пов’язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки [1].

Відповідність стандартам цифрових доказів є дуже важливою, адже електронні дані набагато легше змінити чи підробити, ніж традиційні форми доказів, необхідно дотримуватись правил поводження з даними, які нададуть можливість забезпечити допустимість доказів.

Список використаних джерел:

1. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, 2018. 16 с.

ВОЛОКІТЕНКО Ольга Михайлівна,
доцент кафедри адміністративного
права та адміністративного процесу
Одеського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ НАСИЛЬСТВА В УКРАЇНІ В УМОВАХ ВІЙНИ

Конституція України закріплює, що людина, її життя і здоров’я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю (ст. 3). Від початку повномасштабного російського вторгнення в Україну 24 лютого 2022 року, російські війська були причетними до численних порушень законів і звичаїв війни, які можуть вважатися воєнними злочинами та злочинами проти людства.