досягнень. Ефективне поєднання цих сфер можливе лише за умов дотримання етичних принципів, розвитку правових інститутів і врахування соціально-економічних наслідків, що в сукупності формує основу сталого та відповідального розвитку суспільства.

Література:

1. Бреус, С., & Бондар, А. (2021). Інновації як складова стратегії управління конкурентоспроможністю суб'єкта господарювання. економіка та суспільство, (32). https://doi.org/10.32782/2524-0072/2021-32-106

2. Ганчук, М. (2024). Інновації та їх вплив на економіку сучасного світу. innovation and sustainability, (2), 102–109. https://doi.org/10.31649/ins.2024.2.102.109

3. Крисоватий І. (2024). Концепція інноваційних парків у розвитку економіки. інноваційна економіка, 3, 47-54. https://doi.org/10.37332/

DOI https://doi.org/10.36059/978-966-397-606-8-38

ЦИФРОВІ ДАНІ НСРД І ВИМОГА ЇХ ЗНИЩЕННЯ: ПЕРЕВІРЮВАНІСТЬ ПРОЦЕДУР ЗА СТ. 255 КПК УКРАЇНИ

Романов Віталій Олександрович
кандидат юридичних наук, доцент,
доцент кафедри спеціальних поліцейських дисциплін
та базової загальновійськової підготовки
Сумська філія Харківського національного університету
внутрішніх справ
м. Суми, Україна

У цифровому середовищі проблема знищення невикористаних матеріалів негласних слідчих (розшукових) дій не зводиться до формального видалення файлу. Цифрові дані здатні «повертатися» через резервні копії, журнали доступу, синхронізовані сховища, кеші, тимчасові файли та інші похідні артефакти. У спеціальній літературі неодноразово підкреслюється, що видалення і знищення даних не є тотожними, а основними зонами «виживання» інформації після видалення залишаються резерви та технічні сліди [1; 2]. У контексті невикористаних матеріалів НСРД це свідчить, що навіть належне процесуальне рішення саме по собі не забезпечує досягнення мети ст.

255 КПК України, якщо процедура не охоплює всі місця зберігання даних та їх копії. [3].

З огляду на це поняття «знищення» невикористаних цифрових матеріалів доцільно тлумачити як доведений стан фактичної недоступності змісту та припинення обігу даних у межах органу або інформаційної системи, що забезпечували проведення НСРД. Такий стан не досягається одноразовою операцією «видалення», а потребує комплексу процедур, придатних до перевірки. Вимога ч. 1 ст. 255 КПК України щодо знищення відомостей, речей і документів, які не визнаються необхідними прокурором для досудового розслідування, у цифровому середовищі має реалізовуватися так, щоб унеможливити їх позапроцесуальне використання, а доступ до даних був максимально обмежений [3].

Практичним ядром такого підходу є інвентаризація. Без встановлення того, де саме існують дані, неможливо підтвердити їх фактичне виведення з обігу. Інвентаризація повинна охоплювати основні сховища, архівні контейнери, резервні копії, синхронізовані репозиторії, віддалені копії, а також похідні матеріали, що відтворюють той самий зміст в іншому форматі: витяги, транскрипти, робочі аналітичні довідки. Окрему проблему становлять технологічно необхідні системні журнали, які хоча й виконують службову функцію, але здатні містити чутливі відомості. Тому завданням є не просто «прибрати файл», а забезпечити кероване припинення обігу інформації в усіх контурах її можливого зберігання чи відновлення [1; 2].

Звідси випливає доцільність двоступеневої моделі поводження з невикористаними матеріалами НСРД. Перший етап має охоплювати інвентаризацію місць зберігання та тимчасове блокування доступу до відповідних об’єктів, що мінімізує ризик витоку інформації між моментом прийняття рішення і фактичним знищенням. Другий етап полягає у знищенні даних або припиненні доступу до них з одночасним складанням акта виконання, у якому фіксуються охоплення копій, резервів, синхронізацій, відповідальні особи, час операцій і спосіб контролю [1; 2]. Саме поєднання обмеження доступу та документованого завершення процедури дозволяє перетворити імператив ст. 255 КПК України на реально виконувану гарантію.

Не менш важливим є попередження вторинного використання даних. Нормативна заборона «не використовувати» буде ефективною лише тоді, коли її порушення є технічно складним і залишає сліди в системі. Тому організаційно-технічні бар’єри мають розглядатися як необхідне доповнення до процесуальної норми: рольове розмежування доступу, журналювання перегляду, копіювання та експорту, контроль зовнішніх носіїв і друку, обмеження масового експорту, аудит журналів доступу,

мінімізація копій і регламентація створення похідних матеріалів [4]. Дослідження надійності цифрових криміналістичних процедур свідчать, що документованість, відтворюваність і контроль дотримання стандартів є ключовими передумовами довіри до результатів роботи з цифровими носіями та копіями [4]. Отже, знищення невикористаних матеріалів НСРД має бути не декларацією, а відтворюваною процедурою, здатною витримати перевірку.

Для підвищення підзвітності та одночасного збереження таємниці змісту доцільно забезпечувати перевірюваність на рівні метаданих. Йдеться про фіксацію ідентифікаторів об'єктів без розкриття їх змісту: типу даних, носія або контейнера, часового діапазону, технічних маркерів, місць зберігання, наявності копій і резервів, кола осіб із доступом та способу контролю виконання рішення. Такий підхід дозволяє забезпечити достатній процедурний слід для аудиту без збереження надлишкового приватного змісту. Він узгоджується і з європейськими підходами до оцінки пропорційності втручання у право на приватність, де визначальне значення мають гарантії на етапах зберігання, доступу та знищення отриманих даних [5-7].

На практичному рівні доцільно закріпити мінімальні стандарти документування. По-перше, постанова прокурора про знищення повинна містити реквізити кримінального провадження і правову підставу, перелік об'єктів знищення з ідентифікацією без розкриття змісту, вказівку на місця зберігання, окремий блок щодо копій, резервів і синхронізацій, визначення відповідальних осіб, строк виконання та спосіб контролю [3]. По-друге, уніфікований акт знищення цифрових даних має фіксувати посилання на постанову, повторну ідентифікацію об'єктів, спосіб знищення або припинення доступу, підтвердження охоплення копій, резервів і синхронізацій, час проведення операцій та підписи відповідальних осіб. За можливості до такого акта можуть вноситися технічні маркери перевірюваності, наприклад хеш-ідентифікатор контейнера до знищення, що дозволяє підтвердити ідентичність об'єкта без розкриття його змісту [4].

По-третє, повернення речей і документів повинно супроводжуватися окремим актом приймання-передачі, у якому зазначається, чи створювалися копії або образи цифрових носіїв і якою є їх подальша доля: знищено чи припинено доступ. За відсутності такої фіксації виникає ризик ситуації, коли матеріальний носій повернуто власнику, а його цифровий «двійник» залишається у розпорядженні органу, що суперечить як гарантіям приватності, так і самій логіці ст. 255 КПК України [3]. Водночас знищення невикористаних матеріалів не скасовує обов'язку повідомлення особи про проведення щодо неї НСРД. Тому має зберігатися мінімально необхідний облік метаданих – факт проведення,

часові межі, рішення про необхідність або знищення матеріалів, – достатній для виконання вимог ст. 253 КПК України, але без накопичення надлишкового змісту [3].

Отже, цифровізація зміщує акцент із формального «видалення» на процедурно підтверджене припинення обігу даних і доведення їх фактичної недоступності. Ефективність режиму невикористаних матеріалів НСРД залежить від поєднання правових приписів із технічними та організаційними механізмами контролю. Саме така інтерпретація ст. 255 КПК України дає змогу посилити гарантії приватності, мінімізувати ризик позапроцесуального використання відомостей і забезпечити перевірюваність дій органу, який здійснював НСРД.

Література:

1. Joukov N., Papaxenopoulos H., Zadok E. Secure deletion myths, issues, and solutions. Proceedings of the Second ACM Workshop on Storage Security and Survivability (StorageSS). 2006. DOI: 10.1145/1179559.1179571.

2. Reardon J., Basin D., Čapkun S. SoK: Secure data deletion. 2013 IEEE Symposium on Security and Privacy. 2013. P. 301-315. DOI: 10.1109/SP.2013.28.

3. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI (зі змін.). Ст. 253, 255.

4. Stoykova R., Andersen S., Franke K., Axelsson S. Reliability assessment of digital forensic investigations in the Norwegian police. Forensic Science International: Digital Investigation. 2022. Vol. 40. Article 301351. DOI: 10.1016/j.fsidi.2022.301351.

5. Sommardal J. National security secrecy in ECtHR proceedings-the Court's eroding toolbox against unjustified secrecy and abuse. Human Rights Law Review. 2025. Vol. 25, Issue 3. Article ngaf024. DOI: 10.1093/hrlr/ngaf024.

6. Turanjanin V. When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights approach. International Cybersecurity Law Review. 2023. DOI: 10.1365/s43439-022-00074-7.

7. Zalnieriute M. Big Brother Watch and Others v. the United Kingdom. American Journal of International Law. 2022. Vol. 116, Issue 3. P. 585-592. DOI: 10.1017/ajil.2022.35.