дотримання чітких стандартів щодо автентичності, цілісності та допустимості доказів, а також забезпечення безперервності їх збереження.

Важливим аспектом є також дотримання тактичних і процесуальних вимог під час проведення фото- та відеофіксації, що гарантує їх доказове значення. Необхідність удосконалення нормативного регулювання, уніфікації підходів та впровадження сучасних технічних засобів свідчить про подальший розвиток цієї сфери.

Отже, фото- та відеофіксація виступають невід'ємною та ефективною складовою криміналістичного забезпечення розслідування воєнних злочинів, забезпечуючи належний рівень доказування та сприяючи притягненню винних осіб до відповідальності.

Список використаних джерел

1. Жовтюк О. Міжнародні стандарти криміналістичного забезпечення розслідування воєнних злочинів. *Наука і правоохорона.* 2025. Вип. 4 (70). С. 202–209. DOI: 10.33270/05257004.21

2. Вуйма А. Г. Тактичне забезпечення розслідування воєнних злочинів. *Вісник Кримінологічної асоціації України,* №1(37), С. 5–15.

3. Левицький А. О., Москалюк О. М. Криміналістичне забезпечення розслідування воєнних злочинів: окремі проблеми науково-теоретичних засад. *Криміналістичний вісник.* 2024. № 2 (42), С. 76–85.

4. Філіпов Ю. Техніко-криміналістичне забезпечення розслідування воєнних злочинів: поняття, мета, напрями розвитку. *Реалізація державної антикорупційної політики в міжнародному вимірі :* матеріали VII Міжнар. наук. практ. конф. Київ : Нац. акад. внутр. справ, 2022. С. 296–300.

Цуцкіридзе Максим Сергійович,
доктор юридичних наук, професор,
професор кафедри кримінального процесу
Національної академії внутрішніх справ,
перший заступник Голови Національної
поліції України – начальник Головного
слідчого управління

ЦИФРОВІ СЛІДИ ПРОТИПРАВНОГО ЗАВОЛОДІННЯ ПРОМИСЛОВИМИ ТА СІЛЬСЬКОГОСПОДАРСЬКИМИ ПІДПРИЄМСТВАМИ В УМОВАХ ВОЄННОГО СТАНУ: ВИЯВЛЕННЯ, ЗБЕРЕЖЕННЯ ТА ДОКАЗОВЕ ВИКОРИСТАННЯ

Протиправне заволодіння промисловими та сільськогосподарськими підприємствами в умовах воєнного стану характеризується поєднанням корпоративних, реєстраційних, документальних, фінансових та фактичних способів встановлення незаконного контролю. Закладений у доктрині підхід до рейдерства як складного механізму протиправного перерозподілу власності [1] нині потребує доповнення цифровим компонентом. Зміна відомостей у державних реєстрах, виготовлення електронних документів, використання кваліфікованих електронних підписів, координація учасників через засоби зв'язку та дистанційне управління рахунками залишають цифрові сліди, без дослідження яких неможливо відтворити цілісний механізм посягання.

Цифровий слід у таких провадженнях доцільно розуміти як зафіксоване в інформаційній системі відображення юридично або фактично значущої дії, стану, взаємодії чи події, яке може бути виявлене, належно одержане, збережене, перевірене та використане для встановлення обставин кримінального правопорушення. Йдеться про реєстраційні журнали, історію доступу до облікових записів, електронні документи та їх метадані, серверні журнали, листування, дані мобільних пристроїв, відомості про фінансові операції, геолокаційні дані, резервні копії й інформацію хмарних сервісів. Їх доказове значення визначається не технічною формою як такою, а здатністю підтвердити походження, послідовність і взаємозв'язок дій учасників [5; 8].

Нормативний режим цифрової інформації залишається фрагментарним, тому слідчий має узгоджувати спосіб її одержання з природою об'єкта та ступенем втручання у права особи. Огляд відкритого ресурсу, тимчасовий доступ до речей і документів, обшук, отримання інформації від володільця системи та проведення негласної слідчої (розшукової) дії не є взаємозамінними. Процесуальний спосіб повинен відповідати фактичним умовам доступу, очікуванню приватності й меті втручання, а межі дозволеної дії мають бути визначені заздалегідь [2; 7]. Судовий контроль за такими заходами повинен охоплювати не лише формальну наявність підстав, а й необхідність, пропорційність та достатню конкретизацію шуканих даних [3].

Робота з цифровими слідами має здійснюватися за послідовним алгоритмом: первинне виявлення потенційних джерел; невідкладне запобігання зміні або втраті даних; процесуальне одержання; створення криміналістичної копії; обчислення та фіксація контрольних хеш-значень; документування кожної операції з носієм або копією; аналітичне дослідження; зіставлення з документальними, реєстраційними та фінансовими відомостями; відкриття матеріалів стороні захисту й забезпечення можливості незалежної перевірки. Саме безперервність такого руху утворює ланцюг збереження доказової інформації, порушення якого здатне поставити під сумнів автентичність усього цифрового масиву [10].

У провадженнях щодо заволодіння підприємствами особливого значення набуває збереження контексту цифрової події. Окремий знімок екрана або роздруківка реєстрового запису не завжди дають змогу встановити, хто, коли, з якого облікового запису та з використанням якого технічного засобу вчинив дію. Тому необхідно витребовувати історію змін, журнали автентифікації, дані про сертифікати електронного підпису, часові мітки, IP-адреси та пов'язані службові повідомлення. Законодавство про державну реєстрацію визначає юридичний контекст таких дій [9], але висновок про їх кримінально протиправний характер може бути зроблений лише після зіставлення цифрового запису з корпоративними документами, повноваженнями особи та фактичною спрямованістю поведінки.

Перевірка цифрових даних потребує спеціальних знань. Залучення спеціаліста на етапі пошуку, копіювання та первинної фіксації зменшує ризик втрати метаданих, а судова комп'ютерно-технічна чи інша експертиза дає змогу дослідити властивості об'єкта, відновити видалену інформацію, виявити ознаки втручання та пояснити технічний механізм події [12]. Водночас експертний висновок не замінює процесуального доказування: сторона обвинувачення повинна розкрити походження об'єкта, умови його вилучення, застосовані

інструменти та повний ланцюг передачі, оскільки допустимість залежить від законності й доброчесності процедури одержання доказу [11].

Цифрове доказування не може будуватися за принципом максимально можливого вилучення інформації. Копіювання всього вмісту пристрою або облікового запису без предметного обмеження створює ризик непропорційного втручання у приватність, доступу до професійної таємниці та використання відомостей, не пов'язаних із предметом провадження. Верховенство права вимагає поєднання технологічної ефективності з мінімізацією даних, належним санкціонуванням і реальною можливістю сторони захисту перевірити доказ [4]. Загальні гарантії прав людини у діяльності правоохоронних органів мають діяти на всіх етапах, від первинного доступу до інформації до її судового дослідження [14].

Окремої обережності потребують ситуації, у яких цифрові сліди вказують на використання судової процедури як елемента заволодіння підприємством. Сам факт ухвалення несприятливого або скасованого судового рішення не доводить причетності судді. Необхідна сукупність незалежних даних про позапроцесуальну координацію, усвідомлену спрямованість дій і зв'язок судового акта з реалізацією злочинного плану. Якщо виникають достатні підстави для процесуального реагування щодо судді, повинні неухильно дотримуватися спеціальний порядок повідомлення про підозру та гарантії суддівської незалежності [6]. Матеріали оперативно-розшукової діяльності, що передували такому реагуванню, можуть бути використані лише після належної процесуальної трансформації та перевірки [13].

Отже, цифрові сліди у провадженнях про протиправне заволодіння підприємствами мають розглядатися не як додаток до паперових документів, а як самостійний доказово-інформаційний блок, здатний розкрити послідовність реєстраційних змін, комунікацію співучасників і реальних вигодонабувачів. Його надійність забезпечується сукупністю взаємопов'язаних умов: законним способом одержання, збереженням первинного цифрового середовища, фіксацією хеш-значень і журналу операцій, використанням спеціальних знань, кореляцією з іншими доказами та судовою перевірюваністю. Лише дотримання цих умов дозволяє перетворити технологічну інформацію на допустимий, достовірний і переконливий доказ та водночас не допустити підміни ефективності розслідування необґрунтованим обмеженням прав людини.

Список використаних джерел

1. Кальман О. Г., Погорецький М. А. Рейдерство: причини та заходи протидії. *Вісник Запорізького юридичного інституту Дніпропетровського державного університету внутрішніх справ.* 2009. № 3. С. 150–160.

2. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

3. Погорецький М. А. Судовий контроль та прокурорський нагляд за використанням протоколів оперативно-розшукових заходів як доказів у кримінальному процесі. *Вісник Верховного Суду України.* 2003. № 2. С. 32–38.

4. Погорецький М. А. Забезпечення прав людини в цифровому доказуванні як умова реалізації принципу верховенства права та постановлення справедливого вироку. *Право України.* 2025. № 9. С. 60–74. DOI: https://doi.org/10.33498/louu-2025-09-060. URL: https://pravoua.com.ua/uk/store/pravoukr/pravo_2025_9

5. Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство.* 2025. Т. 3, № 5. С. 239–256. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.37. URL: https://journal-app.uzhnu.edu.ua/article/view/342789

6. Погорецький М. А., Гринюк В. О. Повідомлення судді про підозру: проблемні питання правового регулювання, теорії та практики. *Вісник кримінального судочинства.* 2018. № 2. С. 58–71. URL: https://vkslaw.com.ua/index.php/journal/article/view/272/244

7. Погорецький М. А., Старенький О. С. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України.* 2018. № 8. С. 85–106. URL: http://jnas.nbuv.gov.ua/article/UJRN-0000976271

8. Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури.* 2012. № 8. С. 89–96.

9. Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань: Закон України від 15 трав. 2003 р. № 755-IV. URL: https://zakon.rada.gov.ua/laws/show/755-15#Text

10. Сергєєва Д. Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. Вип. 91. Ч. 4. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/344310

11. Сергєєва Д. Б. Допустимість доказів в теорії та КПК 2012 року. *Вісник кримінального судочинства*. 2015. № 3. С. 80–87. URL: https://vkslaw.com.ua/index.php/journal/article/view/708/625

12. Сергєєва Д. Б. Судові експертизи у кримінальному провадженні : навч. посіб. Київ : Алерта, 2025. 262 с.

13. Шумило М. Є., Погорецький М. А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського інституту внутрішніх справ.* 2001. Вип. 3. С. 199–209.

14. Pogoretskyi M. A., Serhieieva D., Pogoretskyi M. M., Lysachenko Y., Denysenko G. Human rights guarantees in the activities of law enforcement agencies of Ukraine. *Amazonia Investiga*. 2023. Vol. 12, No. 64. P. 249–256. DOI: https://doi.org/10.34069/AI/2023.64.04.24. URL: https://amazoniainvestiga.info/check/64/24-249-256.pdf

Шрамко Дар'я Олександрівна,
здобувач ступеня вищої освіти бакалавра інституту заочного та дистанційного навчання Національної академії внутрішніх справ
Науковий керівник:
доцент кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент ***Семенов В. В.***

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У XXI сторіччі набуває швидкого розвитку інформаційно-технологічний процес. Виникають зовсім нові можливості для кожної людини, нові виклики та нові засоби, які дозволяють облегшити своє життя, заробити грошей або навпаки створюють такі умови, коли людина втрачає все що заробляла довгі роки. Відповідно до цього, кожен інформаційно-технологічний процес має бути врегульований на законодавчому рівні в кожній розвинутій країні.

Особливої уваги потребує дослідження кіберзлочинів в електронних мережах, оскільки з появою нових інформаційно-технологічних процесів,