

***Зразок практичного завдання
для кандидатів на посади старшого аналітика
Відділу цифрової лабораторії Бюро економічної безпеки України***

Опис ситуації (фабула)

Бюро економічної безпеки України (БЕБ) проводить досудове розслідування за фактом підозри у здійсненні схеми ухилення від оподаткування з використанням фіктивних експортних операцій. У межах обшуку офісу підозрюваної компанії вилучено: три ноутбуки співробітників бухгалтерії, робочу станцію головного бухгалтера, чотири USB-накопичувачі, мобільний телефон комерційного директора та зовнішній жорсткий диск, знайдений у сейфі директора.

Матеріали передано Відділу цифрової лабораторії для проведення техніко-криміналістичного дослідження. На момент передання відділ вже має чергу з 14 незавершених досліджень за іншими кримінальними провадженнями; слідчий у цій справі повідомив про процесуальний строк подання висновку — 20 робочих днів.

Під час первинного огляду вилучених носіїв встановлено такі обставини:

- Робоча станція головного бухгалтера має повнодискове шифрування (BitLocker), пароль невідомий; головний бухгалтер відмовляється надавати пароль, посилаючись на право не свідчити проти себе.
- На одному з USB-накопичувачів виявлено видалені файли з розширенням .xlsx; попередній перегляд файлової системи показує, що дані видалено, але не перезаписано.
- Зовнішній жорсткий диск із сейфа має нестандартне розбиття — після стандартного розділу файлова система вказує на «нерозподілений простір», обсяг якого не відповідає сумі видимих розділів.
- На мобільному телефоні комерційного директора встановлено застосунок-гаманець для криптовалюти; у застосунку відображається кілька транзакцій на суму, еквівалентну близько 2,3 млн грн за останні шість місяців.
- Один із ноутбуків бухгалтерії при спробі роботи з ним видав помилку контрольної суми (hash mismatch) під час верифікації образу диска, знятого днем раніше молодшим експертом відділу під час первинного виїзду на місце.
- У відділі наразі працює три експерти (включно з керівником), один із них — новий співробітник з випробувальним терміном, без досвіду роботи з дисковими образами.
- Ліцензія на основний інструмент дослідження мобільних пристроїв обмежена двома робочими станціями одночасно і закінчується через 45 днів; продовження ліцензії вимагає бюджетного запиту, який керівництво БЕБ розглядає раз на квартал.

Керівництву доручено організувати проведення дослідження в межах процесуального строку та підготувати обґрунтовані пропозиції щодо організації роботи.

Завдання

- 1. Чи є відмова головного бухгалтера надати пароль від зашифрованого диска (BitLocker) перешкодою, що унеможливило подальше дослідження цього носія? Які технічні або процесуальні шляхи отримання доступу до даних можливі в такій ситуації? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 2. Яке значення для дослідження має факт, що видалені файли на USB-накопичувачі не було перезаписано? Що це означає для можливості їх відновлення? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 3. Про що може свідчити розбіжність між обсягом «нерозподіленого простору» на зовнішньому диску та сумою видимих розділів? Які подальші дії варто вжити? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 4. Помилка контрольної суми (hash mismatch) під час верифікації образу диска — наскільки це критична проблема для доказової цінності цього образу, і що варто зробити в першу чергу? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 5. Виявлений на телефоні директора криптогаманець з транзакціями на суму, еквівалентну близько 2,3 млн грн, — які додаткові кроки дослідження це відкриває, і чи потрібні для цього інструменти або навички, відмінні від стандартного мобільного форензику? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 6. Черга з 14 незавершених досліджень, строк 20 робочих днів на нову справу, лише 3 експерти (один без досвіду) — як би ви розподілили сім вилучених носіїв цієї справи між наявним персоналом і чому саме так? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 7. Ліцензія на основний інструмент дослідження мобільних пристроїв обмежена двома робочими станціями одночасно і спливає за 45 днів. Як цей факт має вплинути на планування дослідження мобільного телефону директора саме зараз? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 8. Новий співробітник на випробувальному терміні не має досвіду роботи з дисковими образами. Чи варто залучати його до цієї справи, і якщо так — до якої саме частини роботи? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.**
- 9. Якщо до завершення встановленого процесуального строку (20 робочих днів) стає очевидно, що дослідження всіх сімох носіїв завершити неможливо, як варто діяти в цій**

ситуації? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.

10. Яких організаційних чи технічних заходів наразі бракує відділу, судячи з опису черги досліджень і ситуації з ліцензією, щоб уникнути подібних вузьких місць у майбутньому? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.

11. Що з опису обставин цієї справи є підставою для порушення питання про продовження процесуального строку дослідження, а що — ні? Надайте відповідь і наведіть коротке обґрунтування з посиланням на наведені у фабулі обставини.

12. Яку інформацію про хід дослідження кожного носія необхідно фіксувати впродовж роботи, щоб на будь-якому етапі можна було коректно поінформувати слідчого про стан справи? Обґрунтуйте, чому саме ця інформація є ключовою.

Матриця оцінювання практичного завдання

(максимальна оцінка — 100 балів)

- Питання 1 — до 8 балів
- Питання 2 — до 7 балів
- Питання 3 — до 8 балів
- Питання 4 — до 8 балів
- Питання 5 — до 8 балів
- Питання 6 — до 10 балів
- Питання 7 — до 8 балів
- Питання 8 — до 7 балів
- Питання 9 — до 9 балів
- Питання 10 — до 8 балів
- Питання 11 — до 9 балів
- Питання 12 — до 10 балів

Разом: 100 балів