1. Спосіб підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки, за яким здійснюють налаштування агента кінцевої точки таким чином, щоб він знаходився на обчислювальному пристрої кінцевої точки для зв'язку з пристроєм кібербезпеки, налаштування агента кінцевої точки для моніторингу та збору даних про події операційної системи обчислювального пристрою кінцевої точки, пов'язані з кожним файлом з сукупності файлів, що виконуються на обчислювальному пристрої кінцевої точки, налаштування агента кінцевої точки для відправки зібраних даних про події операційної системи через комунікаційний модуль на пристрій кібербезпеки, встановлений у мережі, вибраній з групи, що складається з: і) інформаційно-технологічної мережі; іі) операційної технологічної мережі; ііі) хмарної інфраструктури, де пристрій кібербезпеки містить модель машинного навчання для аналізу даних про події операційної системи обчислювального пристрою кінцевої точки від кожного агента кінцевої точки, підключеного через прикладний програмний інтерфейс до пристрою кібербезпеки, який **відрізняється** тим, що під час збору даних про події операційної системи виконують сукупність знімків змісту файлу у реальному режимі часу, де кожен знімок змісту файлу з сукупності відповідає кожній події операційної системи обчислювального пристрою кінцевої точки, завантажують отриману сукупність знімків змісту файлу за допомогою агента кінцевої точки до пристрою кібербезпеки, де кожен знімок змісту файлу з сукупності має часову мітку, та визначають зміни змісту файлу шляхом порівняння знімків змісту файлу з сукупності за допомогою моделі машинного навчання пристрою кібербезпеки з наступним встановленням часу події операційної системи, яка представляє потенційну загрозу кібербезпеки обчислювального пристрою кінцевої точки.
2. Спосіб за п. 1, який **відрізняється** тим, що події операційної системи обчислювального пристрою кінцевої точки включають запис та читання файлу.
3. Спосіб за п. 1, який **відрізняється** тим, що за допомогою агента кінцевої точки відновлюють зміст файлу, який відповідає змісту файлу до настання події операційної системи, яка представляє потенційну загрозу кібербезпеки обчислювального пристрою кінцевої точки.