УКРАЇНА **(19) UA** **(11) 163872** **(13) U**

(51) МПК
G06N 20/20 (2019.01)

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2026 01432**

(22) Дата подання заявки: **16.03.2026**

(24) Дата, з якої є чинними права інтелектуальної власності: **06.08.2026**

(46) Публікація відомостей про державну реєстрацію: **05.08.2026, Бюл.№ 31**

(72) Винахідник(и):
Мусабєкова Улдана Талгаткизи (AT)

(73) Володілець (володільці):
Мусабєкова Улдана Талгаткизи, Taborstrasse 123/2, 1020, Vienna, Austria (AT)

(74) Представник:
Петренко Сергій Анатолійович, реєстр. №374

(54) СПОСІБ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБЧИСЛЮВАЛЬНОГО ПРИСТРОЮ КІНЦЕВОЇ ТОЧКИ

(57) Реферат:

Спосіб підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки включає 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. 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.

UA 163872 U

Корисна модель належить до систем захисту від кіберзагроз та способів роботи таких систем та може бути використана для підвищення рівня кібербезпеки обчислювальних систем, які працюють у мережевому середовищі, використовуючи з'єднання з одним або кількома віддаленими комп'ютерами/клієнтськими пристроями, такими як віддалені обчислювальні пристрої кінцевої точки.

Захист від кіберзагроз для мережевих обчислювальних пристроїв передбачає виявлення кіберзагроз у режимі реального часу, що передбачають автономне реагування на них з використанням даних про мережу та/або кінцеві пристрої, що дозволяє швидко розслідувати кіберзагрози та усувати їх наслідки. Одним з напрямків зниження ризиків загрози для кібербезпеки є моніторинг цілісності файлів на обчислювальних пристроях кінцевої точки. Актуальним є виявлення зміни вмісту комп'ютерного файлу за допомогою хмарних служб моніторингу цілісності файлів з використанням пристрою кібербезпеки, асоційованого з агентом кінцевої точки, встановленим на обчислювальному пристрої кінцевої точки та конфігурованим для зв'язку з пристроєм кібербезпеки.

Відомо наступні аналогічні способи, серед яких найближчими є наступний, описаний у US2019260785A1 від 22.08.2019 року [https://worldwide.espacenet.com/publicationDetails/biblio?FT=D&date=20190822&DB=EPODOC&locale=en_EP&CC=US&NR=2019260785A1&KC=A1&ND=4]. Спосіб підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки за найближчим аналогом передбачає 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 до прикладного програмного інтерфейсу, розміщеного на пристрої кібербезпеки. За найближчим аналогом збір даних про події операційної системи передбачає відстеження агентом кінцевої точки поведінки процесів (використання мережі, файлової системи тощо), що запускаються на обчислювальному пристрої кінцевої точки, взаємозв'язків між процесами (батьківський/дочірній, спільні файли, міжпроцесна взаємодія) та поведінки користувачів (часто використовувані програми, звички роботи з ІТ). Недоліком способу за найближчим аналогом є відсутність контролю за вмістом файлів, зміна якого може свідчити про наявність шкідливого коду під час їх відкриття, створення або запуску, що в цілому знижує рівень кібербезпеки обчислювального пристрою кінцевої точки.

В основу корисної моделі поставлена задача розробки способу підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки, за яким будуть відстежувати зміну змісту файлу у реальному режимі часу для встановлення часу події операційної системи, яка представляє потенційну загрозу кібербезпеки обчислювального пристрою кінцевої точки.

Поставлена задача вирішується тим, що у відомому способі 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 сукупність прикладних програмних інтерфейсів до пристрою кібербезпеки, згідно з корисною моделлю, 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. Наступним завантажують отриману сукупність знімків змісту файлу за допомогою агента кінцевої точки до пристрою кібербезпеки, де кожен знімок змісту файлу з сукупності має часову мітку. 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.

Технічним результатом є підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки шляхом швидкого визначення зміни змісту файлу, що виконується на обчислювальному пристрої кінцевої точки, та відкату файлу до попередньої історичної версії змісту файлу, збереженої до виникнення потенційного загрози кібербезпеки. Технічний результат досягається використанням служби моніторингу цілісності файлів, виконаної на базі пристрою кібербезпеки з використанням моделі машинного навчання, що дозволяє отримувати та аналізувати різні знімки стану файлів у різні моменти часу, швидко виявляючи шкідливе програмне забезпечення, що ініціювало зміни до файлу, та як змінювався його вміст у реальному часі.

Згідно з одним із варіантів виконання способу, події операційної системи обчислювального пристрою кінцевої точки включають запис та читання файлу, що підвищує надійність визначення кіберзагрози.

Згідно з іншим варіантом виконання способу, 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, що додатково знижує або усуває кіберзагрозу.

Наступним наведено приклад виконання спосіб підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки. Наведений приклад не обмежує інші можливі варіанти виконання способу, а тільки пояснює його суть та підтверджує можливість здійснення.

Спосіб підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки здійснюється за допомогою наступної системи, яка містить обчислювальний пристрій кінцевої точки, агент кінцевої точки, пристрій кібербезпеки, комунікаційний модуль, комп'ютерну мережу, вибрану з групи, що складається з: і) інформаційно-технологічної мережі; іі) операційної технологічної мережі; ііі) хмарної інфраструктури.

Обчислювальним пристроєм кінцевої точки є комп'ютерна система, керована процесором з оперативною пам'яттю та постійним запам'ятовуючим пристроєм, периферійними пристроями, такими як монітор та клавіатура, та обладнана операційною системою для взаємодії користувача з комп'ютерною системою. Комп'ютерна система обирається з ряду систем корпоративного та промислового застосування таких як ноутбук, смартфон, планшет, сервер, термінал збору даних, сканер, POS-термінал, чековий принтер, сканер штрих-кодів. Обчислювальний пристрій кінцевої точки має мережевий інтерфейс для підключення до мережі доступу до Інтернет, який дозволяє пристрою встановлювати мережеву взаємодію з пристроєм кібербезпеки, встановленим у комп'ютерній мережі. Для цього обчислювальний пристрій кінцевої точки має права доступу до вказаної комп'ютерної мережі.

Агентом кінцевої точки є програмний модуль, встановлений на постійний запам'ятовуючий пристрій обчислювального пристрою кінцевої точки та який містить набір машиночитаних інструкцій для виконання процесором. Агент кінцевої точки та пристрій кібербезпеки взаємодіють в режимі клієнт-сервер через комунікаційний модуль, яким обладнано обчислювальний пристрій кінцевої точки, та сукупність прикладних програмних інтерфейсів. До сукупності прикладних програмних інтерфейсів включені стандартні рішення для ведення журналів операційної системи, такі як переадресація подій Windows, Sysmon, а також антивірусні додатки. Агент кінцевої точки та операційна система обчислювального пристрою кінцевої точки взаємодіють через веббраузер, що збережений на постійному запам'ятовуючому пристрої обчислювального пристрою кінцевої точки та який виконується процесором. Через веббраузер також налаштовують доступ агента кінцевої точки до сукупності файлів, що виконуються на обчислювальному пристрої кінцевої точки.

Пристрій кібербезпеки включає такі компоненти, як модуль збору даних, сховище даних, модуль графічного інтерфейсу користувача, мережевий модуль, модуль порівняння, як мінімум один вхідний або вихідний (I/O) порт для безпечного підключення до інших мережевих портів. Модуль графічного інтерфейсу користувача придатний для конфігурації користувачем для вжиття заходів щодо локалізації кіберзагрози. Графічний користувацький інтерфейс пристрою кібербезпеки налаштований для відображення агентів кінцевої точки, підключених до пристрою кібербезпеки. Компоненти пристрою кібербезпеки можуть бути розміщені на обчислювальному пристрої, на одному або декількох серверах або на власній платформі для захисту від кіберзагроз.

Модуль порівняння пристрою кібербезпеки містить принаймні одну з моделей машинного навчання для аналізу даних про події операційної системи від кожного агента кінцевої точки,

підключеного до пристрою кіберзахисту через прикладний програмний інтерфейс. Використовують такі типи моделей машинного навчання, як метрики схожості, кластеризацію, що порівнює структуру даних, класифікаційні моделі або тип нейронних мереж для прямого порівняння двох об'єктів. Для навчання використовують існуючі знімки змісту різних файлів зі змінами, які свідчать про потенційну загрозу кібербезпеки обчислювального пристрою кінцевої точки.

З використанням описаної вище системи налаштовують зв'язок агента кінцевої точки, встановленого на обчислювальному пристрої кінцевої точки, з пристроєм кібербезпеки. За допомогою агента кінцевої точки виконують моніторинг та збір даних про події операційної системи обчислювального пристрою кінцевої точки, пов'язані з кожним комп'ютерним файлом з сукупності файлів, що виконуються на обчислювальному пристрої кінцевої точки. При настанні події операційної системи, наприклад, запис та читання файлу, відправляють зібрані дані про подію через комунікаційний модуль на пристрій кібербезпеки, встановлений у мережі, наприклад, хмарної інфраструктури. Під час збору даних про події операційної системи агент кінцевої точки виконує знімок байтів поточного вмісту файлу, з яким пов'язано подію операційної системи, та який відображає поточний вміст файлу. Кожен знімок змісту файлу відповідає кожній події операційної системи обчислювального пристрою кінцевої точки. Завантажують отриману сукупність знімків змісту файлу за допомогою агента кінцевої точки до пристрою кібербезпеки. Агент кінцевої точки додає часову мітку до кожного знімку змісту файлу у вигляді метаданих, що супроводжують знімки змісту файлу. Наступним порівнюють знімки змісту файлу з сукупності за допомогою моделі машинного навчання пристрою кібербезпеки. Для порівняння використовують байтовий вміст з отриманням згенерованої різниці вмісту як вихідні дані. Як варіант, здійснюють порівняння хеш-значень, що відповідають різному вмісту файлів, наприклад, з використанням алгоритму хешування, де у випадку, коли хеш-значення не є рівними, визначають, що зміст файлу був змінений. Останній варіант порівняння є більш доцільним, оскільки порівняння хеш-значень є простими логічними твердженнями, що потребує менше циклів та менше часу для виявлення підозрілих/шкідливих/аномальних змін файлу. При визначені виявлення підозрілих/шкідливих/аномальних змін у файлі за допомогою часовою мітки встановлюють час події операційної системи, яка представляє потенційну загрозу кібербезпеки обчислювального пристрою кінцевої точки.

Додатково пристрій кібербезпеки надсилає інструкції до агента кінцевого пристрою кібербезпеки кінцевого пристрою для відновлення змісту файлу, який відповідає змісту файлу до настання події операційної системи, відновивши таким чином комп'ютерний файл до раніше збереженої версії. Відновлення здійснюють з використанням попередньо стисненої версії змісту файлу та алгоритмів компресії/декомпресії вихідного змісту файлу.

Таким чином, за допомогою корисної моделі забезпечують підвищення рівня кібербезпеки обчислювального пристрою кінцевої точки.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

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.

Комп'ютерна верстка С. Чулій

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Дмитра Годзенка, 1, м. Київ – 42, 01601