УКРАЇНА **(19) UA** **(11) 157855** **(13) U**

(51) МПК
H04L 41/0894 (2022.01)
H04L 43/04 (2022.01)

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

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2024 02069**
(22) Дата подання заявки: **18.04.2024**
(24) Дата, з якої є чинними права інтелектуальної власності: **05.12.2024**
(46) Публікація відомостей про державну реєстрацію: **04.12.2024, Бюл.№ 49**

(72) Винахідник(и):
Левтеров Андрій Іванович (UA),
Плєхова Ганна Анатоліївна (UA),
Шаронова Наталія Валеріївна (UA),
Неронов Сергій Миколайович (UA)

(73) Володілець (володільці):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ,
вул. Ярослава Мудрого, 25, м. Харків, 61002 (UA)

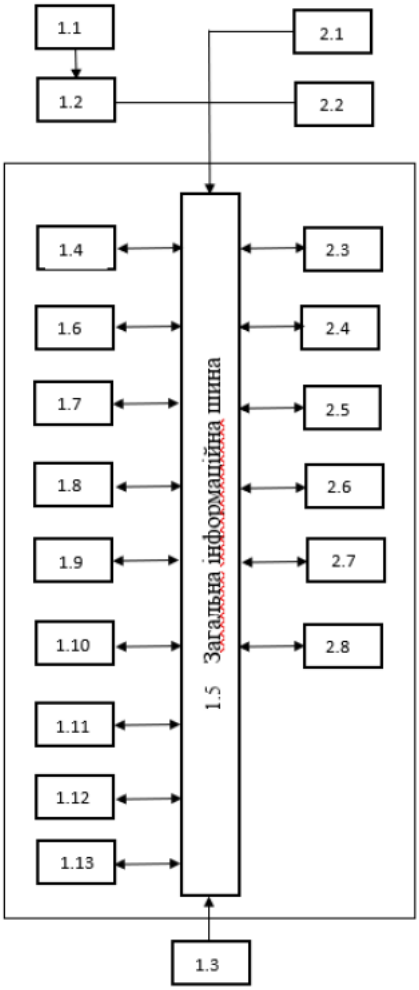
(74) Представник:
Азарова Алла Володимирівна

(54) СИСТЕМА КОНТРОЛЮ ПОЛІТИКИ КІБЕРБЕЗПЕКИ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

(57) Реферат:

Система контролю політики кібербезпеки з застосуванням штучного інтелекту корпоративної мережі зв'язку містить модуль збору даних, засоби зберігання інформації, модуль управління даних, який містить атрибутивний склад елемента інфраструктури, модуль збагачення профілів елементів інфраструктури, що включає інформацію про можливості мережевої взаємодії між активами інфраструктури, на підставі даних правил безпеки, а також правил трансляції та маршрутизації, визначених на мережевих елементах інфраструктури, знайдені уразливості активів інфраструктури, дані про критичність функціонування логічних елементів інфраструктури, відомості про виявлені ризики, а також заходи щодо їх усунення, модуль аналітики, модуль візуалізації, модуль адміністрування, який забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи, модуль інтеграції, модуль збору даних, модуль обробки неструктурованих даних, модуль збору відомостей про встановлене програмне забезпечення, модуль формування структури взаємодії програмного забезпечення між собою, модуль аналізу поверхні захисту, модуль адміністрування. Додатково введені модуль компараторної ідентифікації для отримування можливості та техніки реалізації кожної з відомих комп'ютерних атак та модуль ситуаційно-текстового предикату для виявлення ситуації і сприйняття її залежно від траєкторії реалізації комп'ютерних атак для визначення можливості реалізації кожної з відомих атак і порівняння з можливостями ефективних засобів захисту.

UA 157855 U


1.1
2.1
1.2
2.2
1.4
2.3
1.6
2.4
1.7
2.5
1.8
2.6
1.9
2.7
1.10
2.8
1.11
1.12
1.13
1.5 Загальна інформаційна шина
1.3

Корисна модель належить до обчислювальної техніки та сфери забезпечення інформаційної безпеки.

Відома система інтелектуального управління кіберзагрозами [1], що містить щонайменше один процесор, який забезпечує обробку інформаційних потоків між модулями системи, щонайменше один засіб зберігання даних, що містить машиночитані інструкції, що виконуються процесором, модуль отримання даних, що забезпечує збір інформації із зовнішніх та внутрішніх джерел даних, які містять інформацію про кіберзагрози, фільтрацію отриманих даних та перетворення отриманої інформації в єдиний формат подання, модуль збагачення даних, що забезпечує доповнення даних про індикатори компрометації кіберзагроз із зовнішніх джерел даних, виконання пошуку та збору інформації про шкідливий код, пов'язаний з відомими кіберзагрозами, модуль оновлення інформації про кібербезпеку, що включає щонайменше відомості про вразливість програмного забезпечення, що використовується, про наявність шкідливого коду, пов'язаного з щонайменше однією вразливістю і інформацію про оновлення щонайменше одного програмного забезпечення, що забезпечує захист від щонайменше одного типу вразливості, виявлення облікових записів користувачів, які були задіяні при взаємодії з ресурсами, пов'язаними з індикаторами компрометації, інформація щодо яких зберігається в базі даних, базу даних, що забезпечує зберігання актуальної інформації про кіберзагрози, що передається від модулів отримання даних та модуля збагачення даних, модуль інтеграції, що забезпечує передачу в уніфікованому форматі даних про кіберзагрози у внутрішні джерела, модуль аналітики, що забезпечує виконання аналізу уразливостей IT-інфраструктури у підключених до модуля інтеграції системах, виявлення та відображення неявних зв'язків між інформаційними сутями, що належать до щонайменше одного типу кіберзагрози, за допомогою аналізу ланцюжків зв'язків між згаданими сутями та пошуком загальних вузлів згаданих сутей.

Недоліком цієї системи є низька обґрунтованість формування політики безпеки корпоративної мережі зв'язку через відсутність обліку технік реалізації комп'ютерних мережних атак та взаємозв'язку вразливостей встановленого на елементах інфраструктури програмного забезпечення.

Відома система комп'ютерної безпеки, заснована на штучному інтелекті [2], що характеризується тим, що система комп'ютерної безпеки оснащена пам'яттю і процесором, пов'язаним з пам'яттю, причому дана система комп'ютерної безпеки також включає активний захист критичної інфраструктури за допомогою забезпечення багаторівневого захисту інформації в хмарній архітектурі (CIPR/CTIS), яка додатково включає довірену платформу, що представляє собою мережу агентів, що повідомляють про діяльність хакерів, провайдера керованої мережі та послуг безпеки (MNSP), який забезпечує послуги та рішення щодо керованого безпечного шифрування, підключенням та сумісності, причому MNSP з'єднаний з довіреною платформою за допомогою віртуальної приватної мережі (VPN), яка надає канал зв'язку з довіреною платформою, а MNSP виконаний з можливістю аналізувати весь трафік у мережі підприємства, причому трафік направляють до MNSP, який додатково включає логічний захист і миттєве реагування у реальному часі без створення баз даних (LIZARD), яка дізнається призначення та функцію зовнішнього коду та блокує його у разі наявності злого наміру або відсутності обґрунтованої мети, а також аналізує загрози самі по собі без звернення до минулих даних, штучні загрози безпеці (AST), які являють собою гіпотетичний сценарій події в системі безпеки для перевірки ефективності правил безпеки, творчий модуль, який здійснює процес інтелектуального створення нових гібридних форм із існуючих форм, виявлення злого наміру, з якого визначають взаємозв'язок інформації, виділяють зразки поведінки, що з системою безпеки, проводять регулярні фонові перевірки кількох підозрілих подій у системі безпеки, і навіть роблять спроби знайти взаємозв'язок між подіями, на перший погляд, не пов'язаними між собою, модуль поведінки системи безпеки, в якій зберігаються та індексуються події в системі безпеки, їх ознаки та відгук на них, причому відгуки є рішенням як щодо блокування, так і з допуску, модуль ітеративного зростання та розвитку інтелекту (I2GE), за допомогою якого вивчають великі дані та розпізнають сигнатури шкідливого ПЗ, а також симулюють потенційні різновиди даного ПЗ шляхом поєднання AST з творчим модулем, пам'ять та сприйняття, які засновані на критичному мисленні (CTMP), за допомогою яких критично розглядають рішення щодо блокування або допуску, а також забезпечують додатковий рівень безпеки шляхом вивчення перехресних даних, наданих I2GE, LIZARD та довіреною платформою, причому CTMP оцінює власний потенціал у формуванні об'єктивного рішення з цього питання і не нав'язує це рішення, якщо воно малонадійне.

Недоліком цієї системи є низька обґрунтованість формування політики безпеки корпоративної мережі зв'язку через відсутність обліку технік реалізації комп'ютерних мережних

атак та взаємозв'язку вразливостей встановленого на елементах інфраструктури програмного забезпечення.

Найбільш близьким аналогом за технічною суттю та виконуваним функціям є система контролю політики безпеки елементів корпоративної мережі зв'язку [3], що містить модуль збору даних, що дозволяє отримувати відомості від зовнішніх джерел даних про відомі вразливості елементів інфраструктури та внутрішніх джерел даних про активи інфраструктури мережі зв'язку, засоби зберігання інформації, що дозволяє формувати та зберігати групу структурованих даних, модуля управління даних, що дозволяє нормалізувати дані, що збираються модулем збору даних, забезпечуючи формування уніфікованого виду даних та формування атрибутивного складу залежно від типу елемента інфраструктури, а також формування профілю елемента інфраструктури, що містить атрибутивний склад елемента інфраструктури; модуля збагачення профілів елементів інфраструктури, виконаного з можливістю доповнення атрибутивного складу профілю елемента інфраструктури інформацією, що включає: інформацію про можливості мережевої взаємодії між активами інфраструктури, на підставі даних правил безпеки, а також правил трансляції та маршрутизації, визначених на мережевих елементах інфраструктури, знайдені уразливості активів інфраструктури, дані про критичність функціонування логічних елементів інфраструктури, відомості про виявлені ризики, а також заходи щодо їх усунення, модуля аналітики, що дозволяє враховувати, аналізувати та здійснювати моніторинг зовнішнього периметра мережевої інфраструктури, пошуку за атрибутивним складом профілів активів, аналізу необроблених даних, що надходять із джерел даних управління ризиками за знайденими вразливістю, пошуку та аналізу мережевих маршрутів між активами інфраструктури для визначення можливих шляхів розповсюдження загрози, розрахунку критичності вразливого активу інфраструктури за рахунок визначення впливу вразливостей на мережеву інфраструктуру та її функціонування, а також режиму усунення вразливостей, при якому виявляються активи інфраструктури для усунення знайдених на них вразливостей, модуля візуалізації, що забезпечує графічне подання оброблюваних даних, а також формування віджетів та/або звітів, та/або інформаційних панелей, модуля адміністрування, який забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи; модуля інтеграції, що забезпечує передачу в уніфікованому форматі даних про комп'ютерні атаки у внутрішню інфраструктуру, та забезпечує зв'язок із внутрішніми джерелами даних, модуль збору даних, що дозволяє отримувати відомості від внутрішніх джерел даних про склад та режими роботи засобів захисту від комп'ютерних атак, зовнішніх джерел неструктурованих даних про раніше неописані техніки реалізації комп'ютерних атак та зовнішніх джерел даних про відомі техніки реалізації комп'ютерних атак, модуль обробки неструктурованих даних, що дозволяє за рахунок застосування алгоритмів аналізу тексту виділяти та формувати раніше неописані техніки реалізації комп'ютерних атак із неструктурованих даних, розташованих на спеціалізованих інформаційних ресурсах, модуль збору відомостей про встановлене програмне забезпечення, який здійснює інвентаризацію встановленого програмного забезпечення на кожному засобі обробки, зберігання та передачі інформації, включаючи перелік програмного забезпечення, версії програмного забезпечення, версії отриманого оновлення програмного забезпечення, загальних займаних кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів, модуль формування структури взаємодії програмного забезпечення між собою, що дозволяє на основі визначення загальних зайнятих кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів визначити можливість взаємодії між собою, модуль аналізу поверхні захисту, що дозволяє зіставити відомі вразливості елементів інфраструктури мережі та засоби захисту від комп'ютерних атак, модуль адміністрування, який додатково здійснює формування пропозицій щодо зміни політики безпеки, доповнення засобів захисту, оновлення застосовуваного програмного забезпечення та/або зміни його налаштувань та конфігурації.

Недоліком цієї системи є низька обґрунтованість формування і контролю політики безпеки корпоративної мережі зв'язку через недостатність обліку технік реалізації комп'ютерних мережних атак та взаємозв'язку вразливостей, встановленого на елементах інфраструктури, програмного забезпечення.

В основу корисної моделі поставлена задача розробки системи підвищення обґрунтованості формування і контролю політики кібербезпеки корпоративної мережі зв'язку за рахунок ідентифікації технік реалізації комп'ютерних атак з застосуванням штучного інтелекту та виявлення ситуації і взаємозв'язку вразливостей встановленого на елементах інфраструктури програмного забезпечення.

Поставлена задача вирішується тим, що у систему, що містить модуль збору даних, що дозволяє отримувати відомості від зовнішніх джерел даних про відомі вразливості елементів інфраструктури та внутрішніх джерел даних про активи інфраструктури мережі зв'язку, засоби зберігання інформації, що дозволяє формувати та зберігати групу структурованих даних, модуля управління даних, що дозволяє нормалізувати дані, що збираються модулем збору даних, забезпечуючи формування уніфікованого виду даних та формування атрибутивного складу залежно від типу елемента інфраструктури, а також формування профілю елемента інфраструктури, що містить атрибутивний склад елемента інфраструктури, модуля збагачення профілів елементів інфраструктури, виконаного з можливістю доповнення атрибутивного складу профілю елемента інфраструктури інформацією, що включає інформацію про можливості мережевої взаємодії між активами інфраструктури, на підставі даних правил безпеки, а також правил трансляції та маршрутизації, визначених на мережевих елементах інфраструктури, знайдені уразливості активів інфраструктури, дані про критичність функціонування логічних елементів інфраструктури, відомості про виявлені ризики, а також заходи щодо їх усунення, модуля аналітики, що дозволяє враховувати, аналізувати та здійснювати моніторинг зовнішнього периметра мережевої інфраструктури, пошуку за атрибутивним складом профілів активів, аналізу необроблених даних, що надходять із джерел даних управління ризиками за знайденими вразливістю, пошуку та аналізу мережевих маршрутів між активами інфраструктури для визначення можливих шляхів розповсюдження загрози, розрахунку критичності вразливого активу інфраструктури за рахунок визначення впливу вразливостей на мережеву інфраструктуру та її функціонування, а також режиму усунення вразливостей, при якому виявляються активи інфраструктури для усунення знайдених на них вразливостей, модуля візуалізації, що забезпечує графічне подання оброблюваних даних, а також формування віджетів та/або звітів, та/або інформаційних панелей, модуля адміністрування, який забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи, модуля інтеграції, що забезпечує передачу в уніфікованому форматі даних про комп'ютерні атаки у внутрішню інфраструктуру, та забезпечує зв'язок із внутрішніми джерелами даних, модуль збору даних, що дозволяє отримувати відомості від внутрішніх джерел даних про склад та режими роботи засобів захисту від комп'ютерних атак, зовнішніх джерел неструктурованих даних про раніше неописані техніки реалізації комп'ютерних атак та зовнішні джерела даних про відомі техніки реалізації комп'ютерних атак, модуль обробки неструктурованих даних, що дозволяє за рахунок застосування алгоритмів аналізу тексту виділяти та формувати раніше неописані техніки реалізації комп'ютерних атак із неструктурованих даних, розташованих на спеціалізованих інформаційних ресурсах, модуль збору відомостей про встановлене програмне забезпечення, який здійснює інвентаризацію встановленого програмного забезпечення на кожному засобі обробки, зберігання та передачі інформації, включаючи перелік програмного забезпечення, версії програмного забезпечення, версії отриманого оновлення програмного забезпечення, загальних займаних кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів, модуль формування структури взаємодії програмного забезпечення між собою, що дозволяє на основі визначення загальних зайнятих кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів визначити можливість взаємодії між собою, модуль аналізу поверхні захисту, що дозволяє зіставити відомі вразливості елементів інфраструктури мережі та засоби захисту від комп'ютерних атак, модуль адміністрування, який додатково здійснює формування пропозицій щодо зміни політики безпеки, доповнення засобів захисту, оновлення застосовуваного програмного забезпечення та/або зміни його налаштувань та конфігурації, додатково введені модуль компараторної ідентифікації, який дозволяє отримувати можливості та техніки реалізації кожної з відомих комп'ютерних атак та модуль ситуаційно-текстового предикату для виявлення ситуації і сприйняттям її залежно від траєкторії реалізації комп'ютерних атак, визначити можливість реалізації кожної з відомих атак і порівняти з можливостями ефективних засобів захисту.

На кресленні представлена структурна схема системи контролю політики кібербезпеки з застосуванням штучного інтелекту корпоративної мережі зв'язку.

Система контролю політики кібербезпеки з застосуванням штучного інтелекту корпоративної мережі зв'язку складається з модуля збору даних (1.4), з'єднаного через загальну інформаційну шину (1.5) з зовнішніми джерелами даних (1.2) про відомі вразливості елементів інфраструктури (наприклад, MaxPatrol, Tenable, Qualys, Rapid7 Nexpose, Nmap, Acunetix та ін.), які, у свою чергу, пов'язані з джерелом інформації (1.1), з внутрішніми джерелами даних (1.3) про активи інфраструктури мережі зв'язку (SCCM, uCMDB, HPSM, EMM (Enterprise Mobility Management-AirWatch), AD (Active Directory)), локальні сенсори та ін, з зовнішніми джерелами

неструктурованих даних (2.1) та з зовнішніми джерелами даних про відомі техніки реалізації КА (2.2), з модулем збору відомостей про встановлене програмне забезпечення (2.4), а також із засобом зберігання інформації (1.6).

Засіб зберігання інформації (1.6) через модуль інтеграції (1.12) та загальну інформаційну шину (1.5) надає доступ до модуля управління даними (1.7), модуля збагачення профілів ЕІ (1.8), модуля аналітики (1.9), що дозволяє враховувати, аналізувати та здійснювати моніторинг зовнішнього периметра мережевої інфраструктури, пошуку за атрибутивним складом профілів активів, аналізу необроблених даних, що надходять із джерел даних управління ризиками за знайденими вразливостями, пошуку та аналізу мережевих маршрутів між активами інфраструктури для визначення можливих шляхів розповсюдження загрози, розрахунку критичності вразливого активу інфраструктури за рахунок визначення впливу вразливостей на мережеву інфраструктуру та її функціонування, а також режиму усунення вразливостей, при якому виявляються активи інфраструктури для усунення знайдених на них вразливостей, модулем обробки неструктурованих даних (2.3), модулем формування структури взаємодії програмного забезпечення між собою (2.5), модулем аналізу поверхні захисту (2.6), модулем формування поверхні атаки (2.7).

Модуль компараторної ідентифікації (1.13) через загальну інформаційну шину (1.5) пов'язаний з модулем обробки неструктурованих даних (2.3), а модуль ситуаційно-текстового предикату (2.8) через загальну шину інформації (1.5) пов'язаний з модулем аналізу поверхні захисту (2.6).

Також засіб зберігання інформації (1.6) з'єднаний через загальну інформаційну шину (1.5) з модулем візуалізації (1.10) та модулем адміністрування (1.11) політики безпеки корпоративної мережі зв'язку.

Система контролю політики безпеки елементів корпоративної мережі зв'язку функціонує наступним чином. Із засобів передачі управляючих команд від модуля збору даних із джерел (1.4) на внутрішні джерела даних про активи корпоративної мережі зв'язку (1.3) з метою інвентаризації елементів інфраструктури мережі, які включають відомості про застосовувані засоби обробки, зберігання та передачі інформації, їх технічні характеристики, фізичні та логічні сполуки ЕІ між собою, значення використовуваних інформаційних потоків та пропускної спроможності ліній зв'язку.

Модуль збору відомостей про встановлене програмне забезпечення (2.5) з метою отримання відомостей про встановлене на кожному ЕІ програмне забезпечення, включаючи відомості про версії ПЗ, версії оновлень, загальних займаних кластерів у довгостроковій та оперативній пам'яті, загальних протоколів взаємодії та загальних файлів, а також склад і режими роботи засобів захисту від КА, встановлених на кожному з елементів інфраструктури.

Зовнішні джерела даних про уразливості (1.2) з метою отримання атрибутів описують загальновідомі вразливості інформаційної безпеки (CVE). Зовнішні джерела даних про техніки реалізації КА (2.2) з метою отримання формалізованих відомостей про порядок дій порушника (наприклад, MITRE ATT&CK). Зовнішні джерела про неструктуровані дані про раніше неописані техніки реалізації КА (2.1), наприклад спеціалізованих інформаційних ресурсів (наприклад, SecurityLab.ru, ptsecurity.com, baksdao.com), з метою отримання текстового опису реалізації КА.

Після отримання тестового опису реалізації КА у модулі обробки неструктурованих даних (2.3) з застосуванням компараторної ідентифікації (1.13) виявляють внутрішні структури знайдених предикатів, що характеризують ті чи інші деталі механізму атаки, і далі з використанням спеціалізованого програмного забезпечення розпізнавання та аналізу текстових документів обробляється, зіставляється та створюється формалізоване уявлення реалізації КА у вигляді послідовності вразливостей, що реалізуються. У часі кожна кібератака обмежена тривалістю її спостереження. Атака обмежується також і її спрямованістю. Сприйняття атаки обмежується також рівнем програмного забезпечення та кваліфікацією персоналу, обсягом його знань, спрямованістю його інтересів. У ролі текстів можуть виступати мовні повідомлення, оператори чи команди. Важливо виконати роботу з формального опису перетворення будь-яких повідомлень в тексти, що містяться в них, і далі, застосовуючи алгебру ситуаційно - текстових предикатів (2.8), математично висловити предикати.

Після отримання відомостей про склад встановленого ПЗ на кожному ЕІ та порядок його взаємодії між собою в модулі формування структури взаємодії програмного забезпечення (2.6) формується граф, що репрезентує процес перетворення інформації на моделі взаємодії відкритих систем (МВОС). Вершинами графа є компоненти на кожному з рівнів МВОС, ребрами графа описують можливі процеси взаємодії між ПО. Сформований граф записується у відповідну комірку бази даних.

Після отримання відомостей про склад ЕІ, фізичні та логічні сполуки цих елементів, у модулі аналітики (1.9) формується граф, що відображає переміщення інформації між ЕІ. Сформований граф записується у відповідну комірку бази даних.

Після отримання відомостей про техніку реалізації КА (від зовнішніх джерел даних про КА і модуля обробки неструктурованих даних) в модулі формування поверхні атаки (2.7), кожна з технік зіставляється вразливим, що експлуатуються, наприклад:

T1138: Application Shimming	CVE-2019-0863 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0092 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0091 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0090 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-0088 (Microsoft Windows Elevation of Privilege Vulnerability)
T1144: Rootkit	CVE-2019-1405 (Microsoft Windows Win32k Elevation of Privilege Vulnerability) CVE-2018-1038 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2018-1037 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-7255 (Microsoft Windows Elevation of Privilege Vulnerability) CVE-2016-7254 (Microsoft Windows Elevation of Privilege Vulnerability)
T1170: Mshta	CVE-2017-0199 (Microsoft Office/WordPad Remote Code Execution Vulnerability) CVE-2016-3298 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability) CVE-2016-3297 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability) CVE-2016-3296 (Microsoft Windows Scripting Engine Remote Code Execution Vulnerability)

Після заповнення баз даних про склад ЕІ, структуру мережі, відомі вразливості, застосовуваних засобів захисту від КА та технік реалізації КА, у модулі аналізу поверхні захисту (2.6), сформовані раніше графи доповнюються та уточняються таким чином, що вершини графа зіставляються з базою відомих вразливостей та перейменовуються згідно з класифікацією CVE (всі вершини графа, яким не присвоєна нумерація CVE, виключаються з графа), вага вершини визначається характеристиками застосовуваних засобів захисту, що забезпечують захист на певному рівні МВОС заданого програмного забезпечення від КА, а ребрами графа є переходи між уразливістю під час реалізації відомих технік КА.

Далі у модулі аналітики (1.9) з використанням сформованого у модулі аналізу поверхні захисту (2.6) графа розраховується ймовірність реалізації кожної з відомих КА.

Якщо розраховані значення реалізації КА перевищують допустимі значення, у модулі аналітики (1.9) формують пропозиції щодо застосування додаткових засобів захисту від КА, оновлення застосованого ПЗ та/або зміни налаштувань та режимів роботи ПЗ.

На підставі зібраних внутрішніми джерелами даних про активи (1.3) модуль збагачення профілів ЕІ (1.8) визначає критичність кожного з ЕІ для функціонування ЛЕ та мережі в цілому.

На підставі зібраних зовнішніми джерелами неструктурованих даних (2.1), зовнішніх джерел даних про техніки реалізації КА (2.2) та модуля збору відомостей про встановлене ПЗ (2.4) у модулі збагачення профілів (1.8) формуються базові профілі для кожного ЕІ.

Модуль управління даних (1.7) забезпечує нормалізацію даних та формування профілю атрибутивного складу ЕІ залежно від його типу.

Модуль інтеграції (1.10) забезпечує взаємодію Космосу з джерелами даних.

Модуль візуалізації (1.11) забезпечує подання оброблюваних та збережених у базах даних у вигляді таблиць, графіків, віджетів та/або інформаційних панелей. Модуль візуалізації (1.11) забезпечує формування звітів.

Модуль адміністрування (1.12), що забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи та зокрема забезпечує управління інформацією про користувачів, управління політиками доступу, видачу токенів для доступу до API, управління словниками (облік підмереж периметра та належність їх до територіального блока та FW, Словник програмного забезпечення, який формується за результатами збору профілів активів і наступним накладенням на трубу CVE, що надходить).

Під час експлуатації системи модуль збору даних з джерел (1.1) за допомогою передачі керуючих команд із заданою періодичністю на внутрішні джерела даних про активи мережі (1.3) проводить повторну інвентаризацію мережі з метою виявлення змін у структурі мережі, додавання ЕІ та/або установки ПЗ на ЕІ. У модулі збагачення профілю (1.8) здійснюється порівняння базових профілів ЕІ з профілями ЕІ, що зазнали змін, після чого приймається

рішення про повторні розрахунки в модулі аналізу поверхні захисту (2.6), з подальшими діями в модулі аналітики (1.9).

У ході експлуатації системи модуль збору даних з джерел (1.1) за допомогою передачі керуючих команд із заданою періодичністю на зовнішні джерела даних про вразливості (1.2), зовнішні джерела неструктурованих даних (2.1) і зовнішні джерела даних про техніки реалізації КА (2.2) виявляють зміни в техніках реалізації КА та уточнюють у модулі формування поверхні атаки (2.4) вихідні дані. Крім цього система обробляє та оцінює відомості, включаючи штучний інтелект з застосуванням компараторної ідентифікації (1.13), який дозволить отримувати можливості та техніки реалізації кожної з відомих комп'ютерних атак та з застосуванням ситуаційно-текстового предикату (2.8) для виявлення ситуації з кібератакою і сприйняттям її залежно від траєкторії реалізації комп'ютерних атак, визначити можливість реалізації кожної з відомих атак і порівняти з можливостями ефективних засобів захисту. Уточнені дані обробляються в модулі аналізу поверхні захисту (2.6) і передаються в модуль збагачення профілю (1.8), де здійснюється порівняння базових профілів ЕІ з профілями ЕІ, що зазнали змін, після чого приймається рішення про повторні розрахунки в модулі аналізу поверхні захисту (2.7) з подальшими діями в модулі аналітики (1.9).

Розрахунок ефективності заявленої системи проводився як і в прототипі, а саме - оцінка обґрунтованості проводиться шляхом порівняння коефіцієнтів Тейла для системи прототипу та запропонованої системи [Е.Ю. Піскунов "Модифікація коефіцієнта Тейла". Електронний журнал "Известия Іркутської державної економічної академії", 2012. - № 5.]

$$\nu = \frac{\sqrt{\sum_{i=1}^{T}(P_i - A_i)^2}}{\sqrt{\sum_{i=1}^{T}(A_i)^2}},$$

де Pi та Ai - відповідно, передбачена та фактична (реалізована) зміна змінної. Коефіцієнт v=0, коли все Pi=Ai (випадок досконалого прогнозування), v=1, коли процес прогнозування призводить до тієї ж середньоквадратичної помилки, що і екстраполяція незмінності приростів, v>1, коли прогноз дає гірші результати, ніж припущення про незмінність досліджуваного явища.

Система-прототип додатково обробляє та оцінює відомості про реалізацію КА, що отримані від зовнішніх джерел даних про реалізацію КА та неструктурованих даних, і навіть дані про взаємозв'язок програмного забезпечення встановленого кожного ЕІ, тобто, Pi=3, Ai=6.

Виходячи з цього, коефіцієнт Тейла прийме таке значення:

$$\nu^{\text{прототип}} = \frac{\sqrt{(3-6)^2}}{\sqrt{(6)^2}} = 0,5 .$$

Пропонована система додатково обробляє та оцінює відомості, включаючи штучний інтелект з застосуванням компараторної ідентифікації КІ, який дозволить отримувати можливості та техніки реалізації кожної з відомих комп'ютерних атак та з застосуванням ситуаційно-текстового предикату СТП для виявлення ситуації з кібератакою і сприйняттям її залежно від траєкторії реалізації комп'ютерних атак, визначити можливість реалізації кожної з відомих атак і порівняти з можливостями ефективних засобів захисту, тобто Pi=6, Ai=8.

$$\nu^{\text{система}} = \frac{\sqrt{(3-8)^2}}{\sqrt{(8)^2}} = 0,25 .$$

Далі проводимо порівняння розрахованих коефіцієнтів Тейла для прототипу та заявленої системи

0,25<0,5.

Зі зробленого порівняння розрахованих коефіцієнтів Тейла для системи-прототипу та заявленої системи, висновок, що обґрунтованість формування політики кібербезпеки з елементами штучного інтелекту заявленої системи нижче, ніж у прототипі, що підтверджує досягнення заявленого технічного результату.

Джерела інформації:

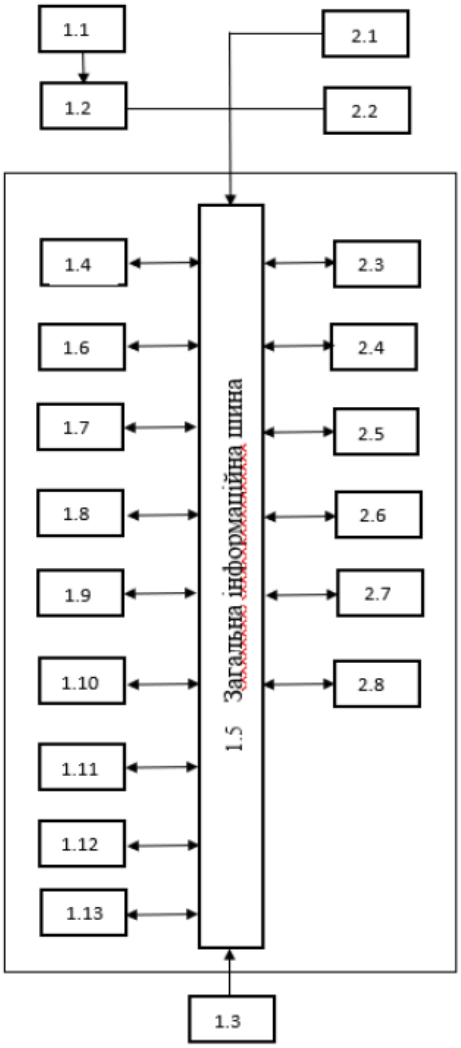
1. Патент RU №2702269 C1, G06F 21/50 (2013.01), G06F 16/22 (2019.01), G06F 7/24 (2006.01). Опубліковано: 07.10.2019 Бюл. № 28. Заявка: 2019117226, 04.06.2019.

2. Патент RU № 2750554 C2, G06N 5/02 (2006.01), G06F 21/50 (2013.01), G06F 21/51 (2013.01), G06F 21/53 (2013.01), G06F 21/54 (2013.01), G06F 21/55 (2013.01), G06F21/56 (2013.01), G06F 21/57 (2013.01). Опубліковано: 29.06.2021 Бюл. № 19. Заявка:2018129947, 24.01.2017.

Патент RU № 2813469 H04L 41/0894 (2022.01), H04L 43/04 (2022.01). Опубліковано: 12.02.2024 Бюл. № 5. Заявка: 2023118355, 12.17.2013.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Система контролю політики кібербезпеки з застосуванням штучного інтелекту корпоративної мережі зв'язку, що містить модуль збору даних, засоби зберігання інформації, модуль управління даних, який містить атрибутивний склад елемента інфраструктури, модуль збагачення профілів елементів інфраструктури, що включає інформацію про можливості мережевої взаємодії між активами інфраструктури, на підставі даних правил безпеки, а також правил трансляції та маршрутизації, визначених на мережевих елементах інфраструктури, знайдені уразливості активів інфраструктури, дані про критичність функціонування логічних елементів інфраструктури, відомості про виявлені ризики, а також заходи щодо їх усунення, модуль аналітики, модуль візуалізації, модуль адміністрування, який забезпечує управління політиками доступу, довідниками, налаштуваннями існуючих модулів системи, модуль інтеграції, модуль збору даних, модуль обробки неструктурованих даних, модуль збору відомостей про встановлене програмне забезпечення, модуль формування структури взаємодії програмного забезпечення між собою, модуль аналізу поверхні захисту, модуль адміністрування, яка **відрізняється** тим, що додатково введені модуль компараторної ідентифікації для отримування можливості та техніки реалізації кожної з відомих комп'ютерних атак та модуль ситуаційно-текстового предикату для виявлення ситуації і сприйняття її залежно від траєкторії реалізації комп'ютерних атак для визначення можливості реалізації кожної з відомих атак і порівняння з можливостями ефективних засобів захисту.



Комп'ютерна верстка Л. Бурлак

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