



УКРАЇНА

(19) **UA** (11) **82020** (13) **U**
(51) МПК (2013.01)
G06F 7/00
G06F 21/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

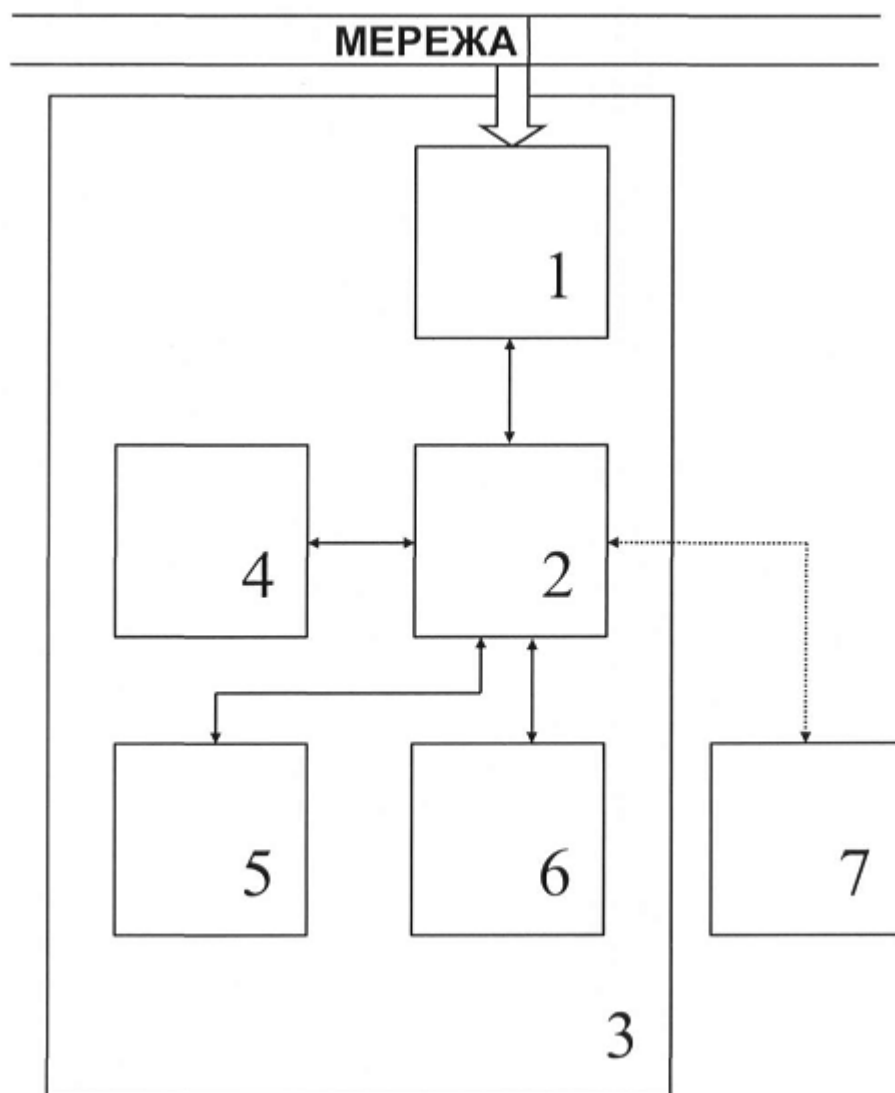
(21) Номер заявки: u 2013 07216	(72) Винахідник(и): Галущенко Олександр Михайлович (UA)
(22) Дата подання заявки: 06.06.2013	(73) Власник(и): Галущенко Олександр Михайлович,
(24) Дата, з якої є чинними права на корисну модель: 10.07.2013	вул. Лановецька, 1, с. Людвинівка,
(46) Публікація відомостей про видачу патенту: 10.07.2013, Бюл.№ 13	Макарівський р-н, Київська обл., 08045 (UA)

(54) СИСТЕМА ДЛЯ МОНІТОРИНГУ, АНАЛІЗУ ТА КОНТРОЛЮ ПОДІЙ БЕЗПЕКИ МЕРЕЖІ

(57) Реферат:

Система для моніторингу, аналізу та контролю подій безпеки мережі містить блок мережевого інтерфейсу, блок програмного управління, блок користувацького інтерфейсу, блок обробки та аналізу інформації, блок збереження інформації, електронно-обчислювальний пристрій. Блок мережевого інтерфейсу виконано з можливістю роботи у режимі promiscuous mode на канальному рівні у мережі по моделі OSI та з можливістю надсилання отриманих пакетів даних через блок програмного управління до блока обробки та аналізу інформації. Блок обробки та аналізу інформації виконано з можливістю фільтрації, кореляційної обробки інформації, створення правил для роботи системи на основі аналізу даних після їх обробки та передачі даних до блока збереження інформації у вигляді оригінальних TCP/IP сесій.

UA 82020 U



Фиг.

Корисна модель належить до систем оброблення цифрових даних за допомогою електричних пристроїв та систем контролю подій безпеки мережі і може бути використана для моніторингу та контролю за внутрішньою мережею, збору даних подій безпеки мережі, їх аналізу за допомогою фільтрації та використання методів кореляції, формування сигналів тривоги та складання звітів про події безпеки мережі.

Найближчим аналогом є система моніторингу, аналізу та зворотної реакції Cisco MARS (Monitoring, Analysis, and Response System), що складається з блока мережевого інтерфейсу, вхід якого з'єднаний з контрольованою мережею, а вихід з блоком програмного управління, що встановлено на електронно-обчислювальному пристрої, блок програмного управління зв'язаний з блоком користувацького інтерфейсу, блоком обробки та аналізу інформації та блоком збереження інформації (Інтернет ресурс http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6241/data_sheet_c78-458671.html).

Відома система моніторингу, аналізу та зворотної реакції Cisco MARS збирає дані про події, що реєструються більшістю розповсюджених мережевих пристроїв (наприклад: маршрутизаторів, комутаторів), пристроїв захисту і програм (наприклад: міжмережеві екрани, системи виявлення вторгнень, сканери вразливості та антивірусні програми) та дозволяє створити топологічну схему мережі, яка містить інформацію про конфігурацію пристроїв та діючих політик безпеки, що дозволяє моделювати потоки пакетів в мережі, здійснити впорядкування отриманих даних з мережі відповідно до топологічної схеми, їх аналізу за допомогою фільтрації та використання методів кореляції. Також система дозволяє блокувати небажані події безпеки мережі та проводити збереження отриманих даних і результатів носії інформації.

Недоліком найближчого аналога є недостатня точність визначення подій безпеки мережі, що знижує надійність та оперативність моніторингу, аналізу та контролю подій безпеки мережі. Крім того, така система моніторингу, аналізу та зворотної реакції не дозволяє здійснити аналіз всіх даних на каналному рівні у мережі по моделі OSI.

В основу корисної моделі поставлено задачу удосконалення системи для моніторингу, аналізу та контролю подій безпеки мережі, в якій за рахунок запропонованого конструктивного виконання елементів забезпечується висока точність визначення подій безпеки мережі при підвищенні надійності та оперативності моніторингу, аналізу та контролю подій безпеки мережі. Крім того, запропоноване виконання системи забезпечує можливість здійснювати аналіз всіх даних на каналному рівні у мережі по моделі OSI.

Поставлена задача вирішується запропонованою системою для моніторингу, аналізу та контролю подій безпеки мережі, що складається з блока мережевого інтерфейсу, вхід якого з'єднаний з контрольованою мережею, а вихід з блоком програмного управління, який зв'язаний з блоком користувацького інтерфейсу, блоком обробки та аналізу інформації та блоком збереження інформації, вказані блоки встановлені на електронно-обчислювальний пристрій, яка включає блок мережевого інтерфейсу, що виконано з можливістю роботи у режимі promiscuous mode на каналному рівні у мережі по моделі OSI та з можливістю надсилання отриманих пакетів даних через блок програмного управління до блока обробки та аналізу інформації, який виконано з можливістю фільтрації, кореляційної обробки інформації, створення правил для роботи системи на основі аналізу даних після їх обробки та передачі даних до блока збереження інформації у вигляді оригінальних TCP/IP сесій.

Для роботи з безпроводними мережами система додатково обладнується блоком для роботи з безпроводними мережами, який виконано з можливістю створення емульованих клієнтів, які під'єднуються до бездротової точки доступу використовуючи декілька наборів характеристик: MAC-адресу, рівень потужності сигналу, час запиту, діапазон таймінгів.

У разі, коли система виконує контроль ділянки мережі, до якої обмежено доступ, блок мережевого інтерфейсу виконаний з можливістю перемикання мережевого інтерфейсу, який підключено до мережі, що контролюється, в розширений promiscuous mode, що здійснюють на каналному рівні моделі OSI, за допомогою сконфігурованого керуючого сигналу, глибина доступності мережевого інтерфейсу, який контролюється та до якого здійснюють підключення і його перемикання, складає від одного до трьох хопів.

Замість власного електронно-обчислювального пристрою система може бути встановлена на електронно-обчислювальний пристрій, наприклад комп'ютер або сервер, який підключено до мережі, що контролюється системою.

Корисна модель пояснюється, але не обмежується кресленням, на якому зображено схематичне зображення системи для моніторингу, аналізу та контролю подій безпеки мережі.

Система для моніторингу, аналізу та контролю подій безпеки мережі включає блок мережевого інтерфейсу 1, блоком програмного управління 2, електронно-обчислювального

пристрою 3, блок користувацького інтерфейсу 4, блок обробки та аналізу інформації 5, блок збереження інформації 6 та може додатково включати блок для роботи з безпроводними мережами 7.

Вхід блока мережевого інтерфейсу 1, що складається з програми управління та мережевого адаптеру, який виконано з можливістю роботи у режимі promiscuous mode на каналному рівні у мережі по моделі OSI, з'єднано з контрольованою мережею, а вихід з'єднано з блоком програмного управління 2. Також блок мережевого інтерфейсу 1 виконано з можливістю надсилання отриманих пакетів даних до блока обробки та аналізу інформації 5. Блок програмного управління 2 з'єднаний з блоком користувацького інтерфейсу 4, блоком обробки та аналізу інформації 5, який виконано з можливістю фільтрації, кореляційної обробки інформації, створення правил на основі аналізу даних після їх обробки та передачі даних до блока збереження інформації 6, утвореного носієм інформації, у вигляді оригінальних TCP/IP сесій. Вказані блоки встановлені на електронно-обчислювальний пристрій 3. Додатково система може бути обладнана блоком для роботи з безпроводними мережами 7, що складається з програми управління та безпроводного мережевого адаптера. Блок для роботи з безпроводними мережами 7 з'єднаний з блоком програмного управління 2. Блок програмного управління 2 керує роботою всіх блоків та системи в цілому.

Система для моніторингу, аналізу та контролю подій безпеки мережі працює наступним чином. Систему, у вигляді електронно-обчислювального пристрою 3, підключають до мережі, що контролюється, під'єднуючи мережевий кабель до входу блока мережевого інтерфейсу 1, який працює в режимі promiscuous mode та виконує надсилання всіх пакетів даних, що передаються на каналному рівні у мережі по моделі OSI до блока програмного управління 2. Блок програмного управління 2 виконує перенаправлення даних до блока обробки та аналізу інформації 5, який виконує фільтрацію, кореляційну обробку інформації, створює правила для роботи системи на основі аналізу даних після їх обробки, та виконує реставрацію даних у їх оригінальному вигляді TCP/IP сесій, які далі передаються до блока збереження інформації 6. Після проведення аналізу інформації блоком обробки та аналізу інформації 5 правила, що були створені для роботи системи передаються до блока програмного управління 2. Контроль за подіями безпеки системи відбувається на основі вказаних правил блоком програмного управління 2. Також, блок програмного управління 2, може передавати отримані дані з блока мережевого інтерфейсу 1 до блока збереження інформації 6 для їх архівування та подальшої обробки за допомогою блока обробки та аналізу інформації 5. У разі, коли система працює з мережею, доступ до якої може бути здійснено тільки через бездротову точку доступу, до блока програмного управління додатково приєднується блок для роботи з безпроводними мережами 7, що створює емульованих клієнтів, які під'єднується до бездротової точки доступу використовуючи декілька наборів характеристик: MAC-адресу, рівень потужності сигналу, час запиту, діапазон таймінгів до тих пір, поки не почнеться взаємодія клієнта та бездротової точки доступу, що видає сервісне повідомлення, необхідне для з'єднання на апаратному рівні, після чого запускається процедура обміну технічною інформацією, що містить дані, необхідні для підключення клієнта, та відбувається обробка інформації контролюючим пристроєм потрібної для аудиту мережі. Результатом роботи системи є структуровані дані збережені на носій інформації, що можуть бути виведені на екран електронно-обчислювального пристрою за допомогою блока користувацького інтерфейсу у їх оригінальному вигляді або використані як матеріал для аналізу блоком обробки та аналізу інформації 5.

Таким чином, запропонована система для моніторингу, аналізу та контролю подій безпеки мережі забезпечує високу точність визначення подій безпеки мережі при підвищенні надійності та оперативності моніторингу, аналізу та контролю подій безпеки мережі. Крім того, система забезпечує можливість здійснювати аналіз всіх даних на каналному рівні у мережі по моделі OSI.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

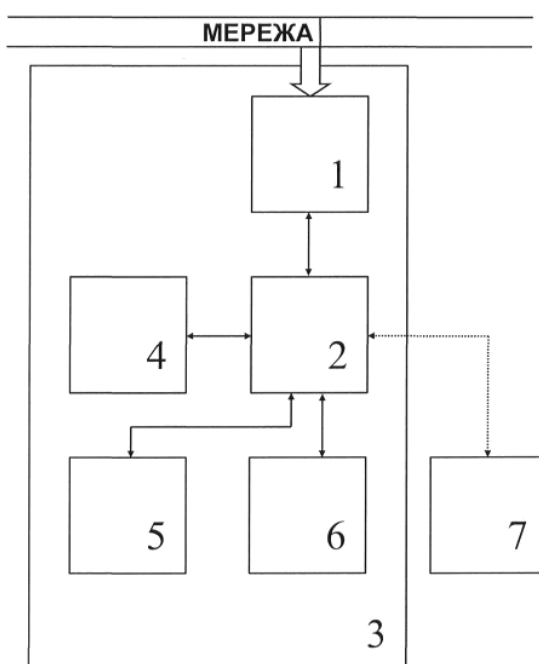
1. Система для моніторингу, аналізу та контролю подій безпеки мережі, що складається з блока мережевого інтерфейсу, вхід якого з'єднаний з контрольованою мережею, а вихід з блоком програмного управління, який зв'язаний з блоком користувацького інтерфейсу, блоком обробки та аналізу інформації та блоком збереження інформації, вказані блоки встановлені на електронно-обчислювальний пристрій, яка **відрізняється** тим, що блок мережевого інтерфейсу виконано з можливістю роботи у режимі promiscuous mode на каналному рівні у мережі по моделі OSI та з можливістю надсилання отриманих пакетів даних через блок програмного управління до блока обробки та аналізу інформації, який виконано з можливістю фільтрації,

кореляційної обробки інформації, створення правил для роботи системи на основі аналізу даних після їх обробки та передачі даних до блока збереження інформації у вигляді оригінальних TCP/IP сесій.

2. Система за п. 1, яка **відрізняється** тим, що блок програмного управління додатково обладнано блоком для роботи з безпроводними мережами, який виконано з можливістю створення емульованих клієнтів, які під'єднуються до бездротової точки доступу, використовуючи декілька наборів характеристик: MAC-адресу, рівень потужності сигналу, час запиту, діапазон таймінгів.

3. Система за п. 1, яка **відрізняється** тим, що блок мережевого інтерфейсу виконаний з можливістю перемикання мережевого інтерфейсу, який підключено до мережі, що контролюється, в розширений promiscuous mode, що здійснюють на канальному рівні моделі OSI, за допомогою сконфігурованого керуючого сигналу, глибина доступності мережевого інтерфейсу, який контролюється та до якого здійснюють підключення і його перемикання, складає від одного до трьох хопів.

4. Система за п. 1, яка **відрізняється** тим, що як електронно-обчислювальний пристрій використовують електронно-обчислювальний пристрій, який підключено до мережі, що контролюється системою.



Комп'ютерна верстка А. Крижанівський

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601