УКРАЇНА

(19) UA (11) 154558 (13) U

(51) МПК (2023.01)
H04B 10/00
H04B 15/00

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

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2023 02083**

(22) Дата подання заявки: **02.05.2023**

(24) Дата, з якої є чинними права інтелектуальної власності: **23.11.2023**

(46) Публікація відомостей про державну реєстрацію: **22.11.2023, Бюл.№ 47**

(72) Винахідник(и):
Шемендюк Олександр Віталійович (UA),
Богдан Володимир Миколайович (UA),
Чередниченко Олексій Юрійович (UA),
Процюк Юрій Олександрович (UA),
Ляшенко Ганна Тарасівна (UA),
Гаврилюк Оксана Григорівна (UA),
Фомкін Денис Валентинович (UA)

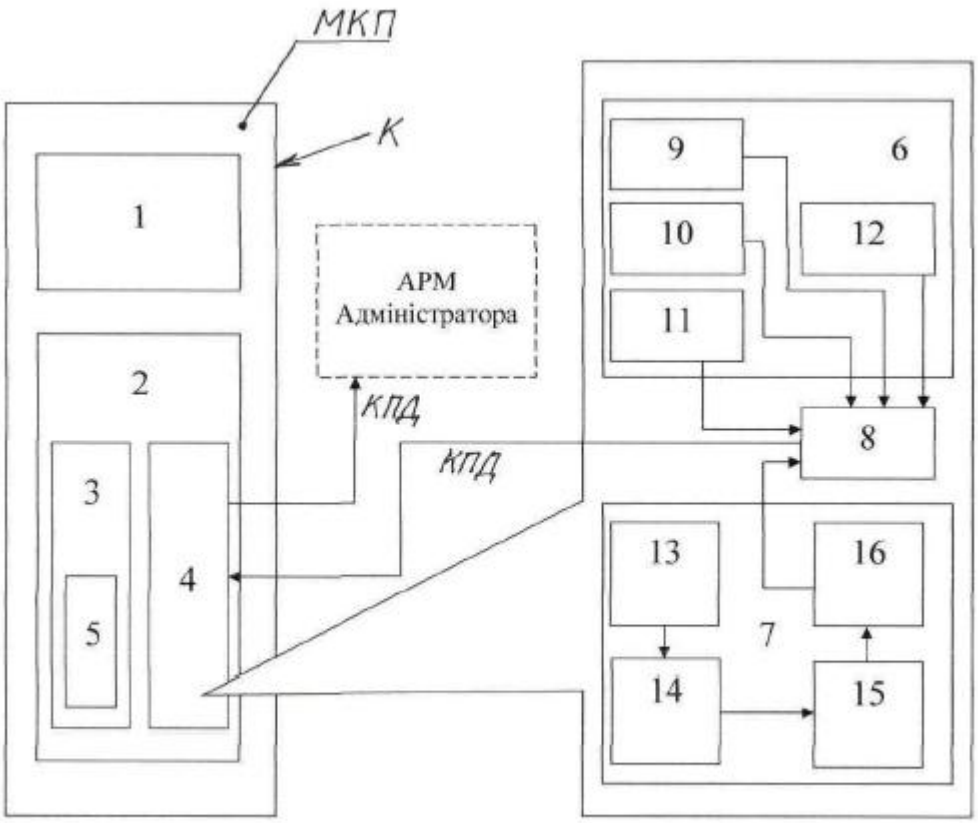
(73) Володілець (володільці):
Шемендюк Олександр Віталійович,
вул. Срібнокільська, 20, кв. 248, м. Київ, 02095 (UA)

(54) МОБІЛЬНИЙ КОМУНІКАЦІЙНИЙ ПРИСТРІЙ

(57) Реферат:

Мобільний комунікаційний пристрій містить корпус із розміщеними у ньому технічними засобами, програмним забезпеченням та каналами передачі даних, при цьому до складу програмного забезпечення входить загальне програмне забезпечення і спеціальне програмне забезпечення, причому до складу загального програмного забезпечення входить система захисту. До складу спеціального програмного забезпечення додатково введені система управління мобільним комунікаційним пристроєм, система моніторингу і реагування на кіберінциденти, блок передачі інформації. При цьому до складу системи управління мобільним комунікаційним пристроєм входять підсистема контролю мобільних додатків, підсистема віддаленого налаштування, підсистема шифрування даних і підсистема віддаленого управління, до складу системи моніторингу і реагування на кіберінциденти входять підсистема моніторингу і збору інформації, підсистема аналізу даних, підсистема реагування на кіберінциденти і підсистема оповіщення. Причому виходи підсистеми контролю мобільних додатків, підсистеми віддаленого налаштування, підсистеми шифрування даних і підсистеми віддаленого управління, що входять до складу системи управління мобільним комунікаційним пристроєм, з'єднано, відповідно, з першим, другим, третім та четвертим входами блока передачі інформації. Вихід підсистеми моніторингу і збору інформації, що входить до складу системи моніторингу і реагування на кіберінциденти, з'єднано послідовно через підсистему аналізу даних і підсистему реагування на кіберінциденти з входом підсистеми оповіщення, вихід якої з'єднано з п'ятим входом блока передачі інформації. Вихід блока передачі інформації з'єднано з входом спеціального програмного забезпечення, а вихід спеціального програмного забезпечення з'єднано каналами передачі даних з автоматизованим робочим місцем адміністратора.

UA 154558 U


МКП
К
1
2
3
4
5
АРМ
Адміністратора
КПД
КПД
9
6
10
12
11
8
13
16
7
14
15

Фіг. 2

Корисна модель належить до галузі радіотехніки, зокрема до засобів обміну інформацією, а саме, до мобільних комунікаційних пристроїв і може бути використана для захисту інформації мобільного комунікаційного пристрою.

Умови XXI століття передбачають часте використання інформаційних технологій та гаджетів. І одним з найпоширеніших, щоденним супутником кожної людини є мобільний телефон. Проте, з ростом використання смарт-пристроїв, зростає і небезпека витоку та втрати даних. Саме тому кожному користувачеві варто подбати про належний рівень безпеки (кібербезпеки) мобільних комунікаційних пристроїв [1].

Всі мобільні комунікаційні пристрої дозволяють власнику самостійно їх налаштовувати (адмініструвати) згідно з опціями за моделями пристроїв та за версіями операційних систем для забезпечення захисту даних на них [2]. Тобто власник мобільного комунікаційного пристрою може власними силами налаштувати його для безпечної роботи.

Виконання рекомендацій щодо забезпечення його захищеності покладається на сумління власника мобільного комунікаційного пристрою та залежить від його відповідальності, що не може в повній мірі забезпечити його захищеність та своєчасне реагування на інциденти безпеки [3].

Відомий мобільний комунікаційний пристрій, що містить корпус із розміщеними у ньому технічними засобами, програмним забезпеченням та каналами передачі даних, при цьому як технічні засоби використаний екран та клавіатура, до складу програмного забезпечення входить загальне програмне забезпечення і спеціальне програмне забезпечення, причому до складу загального програмного забезпечення входить система захисту [4].

До недоліків відомого мобільного комунікаційного пристрою належить те, що:

- вся відповідальність за захист інформації мобільного комунікаційного пристрою залежить лише від користувача мобільного комунікаційного пристрою;
- відсутність централізованого налаштування та управління мобільним комунікаційним пристроєм;
- відсутність своєчасного аналізу та реагування на кіберінциденти.

Таким чином, тим обладнанням, що входить до складу мобільного комунікаційного пристрою, неможливо забезпечити повноцінну захищеність мобільного комунікаційного пристрою, оскільки існуюча система захисту операційної системи мобільного комунікаційного пристрою не може в повній мірі забезпечити безпеку даних мобільного комунікаційного пристрою та своєчасне реагування на кіберінциденти.

Найбільш близьким технічним рішенням як за суттю, так і за задачею, що вирішується, яке вибрано за найближчий аналог (прототип), є мобільний комунікаційний пристрій, що містить корпус із розміщеними у ньому технічними засобами, програмним забезпеченням та каналами передачі даних, при цьому до складу програмного забезпечення входить загальне програмне забезпечення і спеціальне програмне забезпечення, причому до складу загального програмного забезпечення 3 входить система захисту [5].

До недоліків відомого мобільного комунікаційного пристрою, який вибрано за найближчий аналог (прототип), належить те, що:

- вся відповідальність за захист інформації мобільного комунікаційного пристрою залежить лише від користувача мобільного комунікаційного пристрою;
- відсутність централізованого налаштування та управління мобільним комунікаційним пристроєм;
- відсутність своєчасного аналізу та реагування на кіберінциденти.

Таким чином, тим обладнанням, що входить до складу мобільного комунікаційного пристрою, який вибрано за найближчий аналог (прототип), не може в повній мірі забезпечити захищеність мобільного комунікаційного пристрою, оскільки існуюча система захисту операційної системи мобільного комунікаційного пристрою не може в повній мірі забезпечити безпеку даних мобільного комунікаційного пристрою та своєчасне реагування на кіберінциденти.

В основу корисної моделі поставлена задача шляхом введення до складу спеціального програмного забезпечення, що входить до складу мобільного комунікаційного пристрою, додатково системи управління мобільним комунікаційним пристроєм, системи моніторингу і реагування на кіберінциденти та блока передачі інформації, забезпечити підвищення захищеності зазначеного мобільного комунікаційного пристрою.

Поставлена задача вирішується тим, що мобільний комунікаційний пристрій містить корпус із розміщеними у ньому технічними засобами, програмним забезпеченням та каналами передачі даних, при цьому до складу програмного забезпечення входить загальне програмне забезпечення і спеціальне програмне забезпечення, причому до складу загального програмного

забезпечення входить система захисту, згідно з корисною моделлю до складу спеціального програмного забезпечення 4 додатково введені система управління мобільним комунікаційним пристроєм, система моніторингу і реагування на кіберінциденти, блок передачі інформації, при цьому до складу системи управління мобільним комунікаційним пристроєм входять підсистема контролю мобільних додатків, підсистема віддаленого налаштування, підсистема шифрування даних і підсистема віддаленого управління, до складу системи моніторингу і реагування на кіберінциденти входять підсистема моніторингу і збору інформації, підсистема аналізу даних, підсистема реагування на кіберінциденти і підсистема оповіщення, причому виходи підсистеми контролю мобільних додатків, підсистеми віддаленого налаштування, підсистеми шифрування даних і підсистеми віддаленого управління, що входять до складу системи управління мобільним комунікаційним пристроєм, з'єднано, відповідно, з першим, другим, третім та четвертим входами блока передачі інформації, вихід підсистеми моніторингу і збору інформації, що входить до складу системи моніторингу і реагування на кіберінциденти, з'єднано послідовно через підсистему аналізу даних і підсистему реагування на кіберінциденти з входом підсистеми оповіщення, вихід якої з'єднано з п'ятим входом блока передачі інформації, вихід блока передачі інформації з'єднано з входом спеціального програмного забезпечення, а вихід спеціального програмного забезпечення з'єднано каналами передачі даних з автоматизованим робочим місцем адміністратора.

Порівняльний аналіз технічного рішення, що заявляється, з прототипом, дозволяє зробити висновок, що мобільний комунікаційний пристрій, що заявляється, відрізняється тим, що до складу спеціального програмного забезпечення додатково введені система управління мобільним комунікаційним пристроєм, система моніторингу і реагування на кіберінциденти та блок передачі інформації, до складу системи управління мобільним комунікаційним пристроєм входять підсистема контролю мобільних додатків, підсистема віддаленого налаштування, підсистема шифрування даних і підсистема віддаленого управління, до складу системи моніторингу і реагування на кіберінциденти входять підсистема моніторингу і збору інформації, підсистема аналізу даних, підсистема реагування на кіберінциденти і підсистема оповіщення, виходи підсистеми контролю мобільних додатків, підсистеми віддаленого налаштування, підсистеми шифрування даних і підсистеми віддаленого управління, що входять до складу системи управління мобільним комунікаційним пристроєм, з'єднано, відповідно, з першим, другим, третім та четвертим входами блока передачі інформації, вихід підсистеми моніторингу і збору інформації, що входить до складу системи моніторингу і реагування на кіберінциденти, з'єднано послідовно через підсистему аналізу даних і підсистему реагування на кіберінциденти з входом підсистеми оповіщення, вихід якої з'єднано з п'ятим входом блока передачі інформації, вихід блока передачі інформації з'єднано з входом спеціального програмного забезпечення, а вихід спеціального програмного забезпечення з'єднано каналами передачі даних з автоматизованого робочого місця адміністратора.

Суть корисної моделі пояснюють креслення.

На фіг. 1 показано блок-схему конструктивного виконання мобільного комунікаційного пристрою, що вибрано за найближчий аналог.

На фіг. 2 показано блок-схему конструктивного виконання мобільного комунікаційного пристрою, що заявляється, що з'єднаний каналами передачі даних з автоматизованим робочим місцем адміністратора.

Мобільний комунікаційний пристрій (поз. "МКП"), що заявляється, містить (як варіант конструктивного виконання) корпус (поз. "К") із розміщеними у ньому технічними засобами 1, програмним забезпеченням 2 та каналами (поз. "КПД") передачі даних, при цьому до складу програмного забезпечення 2 входить загальне програмне забезпечення 3 і спеціальне програмне забезпечення 4, причому до складу загального програмного забезпечення 3 входить система захисту 5 (див. блок-схему на фіг. 1).

Конструктивно до складу спеціального програмного забезпечення 4 також входять (див. блок-схему на фіг. 2):

- система 6 управління мобільним комунікаційним пристроєм,
- система 7 моніторингу і реагування на кіберінциденти,
- блок 8 передачі інформації,

Конструктивно до складу системи 6 управління мобільним комунікаційним пристроєм входять:

- підсистема 9 контролю мобільних додатків,
- підсистема 10 віддаленого налаштування,
- підсистема 11 шифрування даних,
- підсистема 12 віддаленого управління.

Конструктивно до складу системи 7 моніторингу і реагування на кіберінциденти входять:
- підсистема 13 моніторингу і збору інформації,
- підсистема 14 аналізу даних,
- підсистема 15 реагування на кіберінциденти,
- підсистема 16 оповіщення.

Конструктивно і технологічно у мобільному комунікаційному пристрої (поз. "МКП"), що заявляється, його складові з'єднано між собою таким чином:

- виходи підсистеми 9 контролю мобільних додатків, підсистеми 10 віддаленого налаштування, підсистеми 11 шифрування даних і підсистеми 12 віддаленого управління, що входять до складу системи 6 управління мобільним комунікаційним пристроєм, з'єднано, відповідно, з першим, другим, третім та четвертим входами блока 8 передачі інформації,
- вихід підсистеми 13 моніторингу і збору інформації, що входить до складу системи 7 моніторингу і реагування на кіберінциденти, з'єднано послідовно через підсистему 14 аналізу даних і підсистему 15 реагування на кіберінциденти з входом підсистеми 16 оповіщення,
- вихід підсистеми 16 оповіщення з'єднано з п'ятим входом блока 8 передачі інформації,
- вихід блока 8 передачі інформації з'єднано з входом спеціального програмного забезпечення 4,
- вихід спеціального програмного забезпечення 4 з'єднано каналами (поз. "КПД") передачі даних з автоматизованим робочим місцем адміністратора (поз. "АРМ") - див. блок-схему на фіг. 2.

Мобільний комунікаційний пристрій (поз. "МКП"), що заявляється, працює таким чином.

Попередньо у корпусі (поз. "К") мобільного комунікаційного пристрою (поз. "МКП"), що заявляється, розміщують наступні складові елементи: - технічні засоби 1 та програмне забезпечення 2 (до складу якого входить загальне програмне забезпечення 3 і спеціальне програмне забезпечення 4, причому до складу загального програмного забезпечення 3 входить система захисту 5) - (див. блок-схему на фіг. 1).

Після цього до складу спеціального програмного забезпечення 4 додатково вводять (див. блок-схему на фіг. 2):

- систему 6 управління мобільним комунікаційним пристроєм (до складу якої входять підсистема 9 контролю мобільних додатків, підсистема 10 віддаленого налаштування, підсистема 11 шифрування даних та підсистема 12 віддаленого управління),
- систему 7 моніторингу і реагування на кіберінциденти (до складу якої входять підсистема 13 моніторингу і збору інформації, підсистема 14 аналізу даних, підсистема 15 реагування на кіберінциденти та підсистема 16 оповіщення).
- блок 8 передачі інформації (див. блок-схему на фіг. 2).

Конструктивно і технологічно у мобільному комунікаційному пристрої (поз. "МКП"), що заявляється, його складові з'єднують між собою таким чином:

- виходи підсистеми 9 контролю мобільних додатків, підсистеми 10 віддаленого налаштування, підсистеми 11 шифрування даних і підсистеми 12 віддаленого управління, що входять до складу системи 6 управління мобільним комунікаційним пристроєм, з'єднують, відповідно, з першим, другим, третім та четвертим входами блока 8 передачі інформації,
- вихід підсистеми 13 моніторингу і збору інформації, що входить до складу системи 7 моніторингу і реагування на кіберінциденти, з'єднують послідовно через підсистему 14 аналізу даних і підсистему 15 реагування на кіберінциденти з входом підсистеми 16 оповіщення,
- вихід підсистеми 16 оповіщення з'єднують з п'ятим входом блока 8 передачі інформації,
- вихід блока 8 передачі інформації з'єднують з входом спеціального програмного забезпечення 4.

Технологічно в структурі мобільного комунікаційного пристрою (поз. "МКП"), що заявляється, передбачено канали (поз. "КПД") передачі даних, за допомогою яких вихід спеціального програмного забезпечення 4 буде з'єднаним (при роботі мобільного комунікаційного пристрою (поз. "МКП"), що заявляється) з автоматизованим робочим місцем адміністратора (поз. "АРМ") - див. блок-схему на фіг. 2.

Підготовлений таким чином мобільний комунікаційний пристрій, що заявляється, використовується (працює), для підвищення його захищеності, наступним чином.

Мобільний комунікаційний пристрій по каналах (поз. "КПД") передачі даних отримує вхідні сигнали технічними засобами 1, передає програмному забезпеченню 2. Загальне програмне забезпечення 3 обробляє отримані дані власними вбудованими засобами або передає на обробку спеціальному програмному забезпеченню 4. З автоматизованого робочого місця адміністратора (поз. "АРМ" - див. фіг. 2) налаштовуються підсистема 9 контролю мобільних додатків та підсистема 11 шифрування даних системи 6 управління мобільного комунікаційного

пристрою (поз. "МКП"), та система 7 моніторингу і реагування на кіберінциденти через блок 8 передачі інформації. Дані, які надходять до програмного забезпечення 2 проходять через підсистему 13 моніторингу і збору інформації, аналізуються підсистемою 14 аналізу даних і за допомогою підсистеми 15 реагування на кіберінциденти проходить відповідна реакція на кіберінцидент з негайним оповіщенням адміністратора (поз. "АРМ") через підсистему 16 оповіщення. У випадку необхідності виконання певних дій з мобільним комунікаційним пристроєм (поз. "МКП"), адміністратор (поз. "АРМ") через підсистему 10 віддаленого налаштування та підсистему 12 віддаленого управління системи 6 управління мобільного комунікаційного пристрою (поз. "МКП") вживає необхідних заходів для забезпечення безпеки даних та відповідно підвищення захищеності мобільного комунікаційного пристрою.

Таким чином здійснюється централізоване налаштування та захист мобільного комунікаційного пристрою, що в повній мірі забезпечує безпеку даних мобільного комунікаційного пристрою та своєчасне реагування на кіберінциденти.

Підвищення ефективності застосування мобільного комунікаційного пристрою, що заявляється, у порівнянні з прототипом, досягається шляхом введення до складу спеціального програмного забезпечення, що входить до складу мобільного комунікаційного пристрою, додатково системи управління мобільним комунікаційним пристроєм, системи моніторингу і реагування на кіберінциденти та блока передачі інформації, чим забезпечують підвищення захищеності зазначеного мобільного комунікаційного пристрою.

ДЖЕРЕЛА ІНФОРМАЦІЇ:

1. https://datami.ua/bezpeka-i-kiberbezpeka-smartfoniv/.

2. https://24tv.ua/tech/sekreti-androyid-9-nalashtuvan-yaki-novini-mobilnih-telefoniv_n1829772.

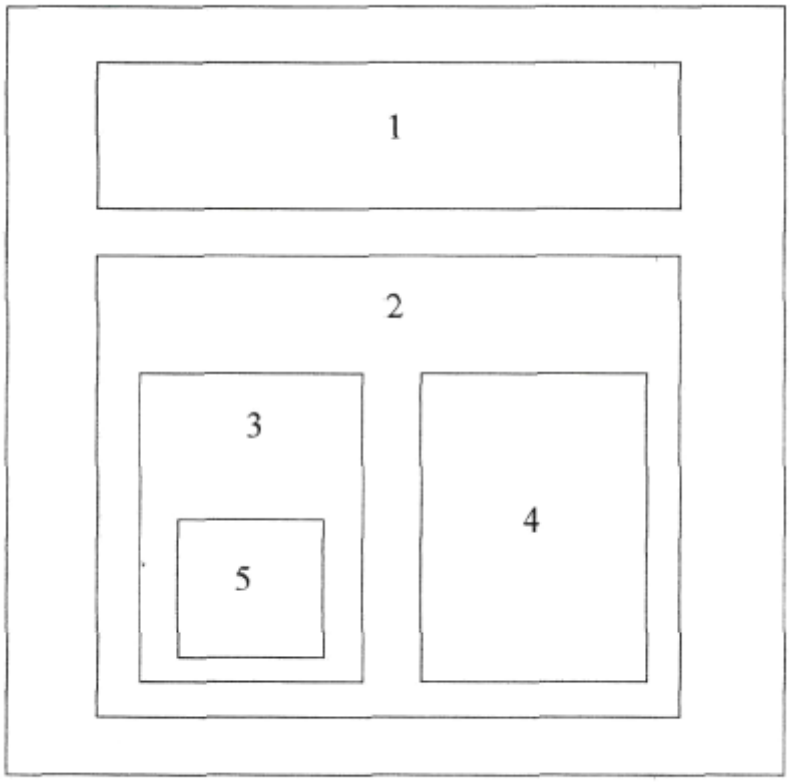
3. httpsi//www.samsung.com/ua/support/mobile-devices/what-viruses-can-affect-android-and-how-to-remove-them/.

4. Мобільний комунікаційний пристрій [Інтернет ресурс] https://hddrecover.ru/total/vse-o-smartfone-chto-eto-takoe-i-kak-on-rabotaet-plyusy-i-minusy-telefona/ - аналог.

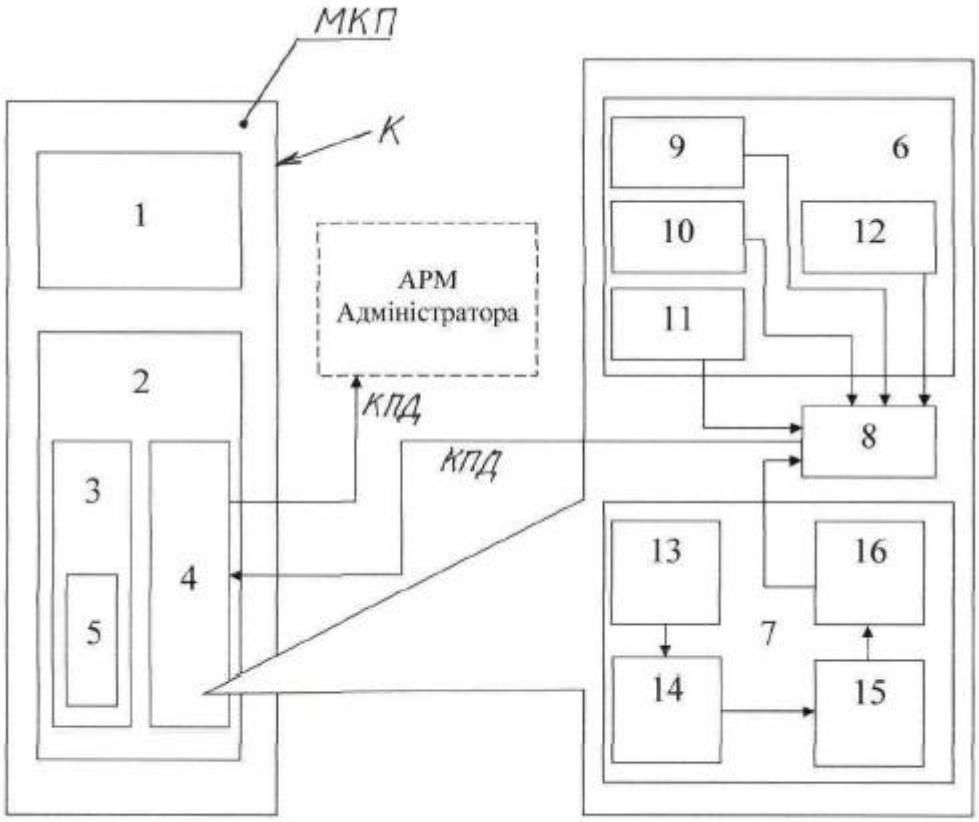
5. Мобільний комунікаційний пристрій [Інтернет ресурс] http://gsm-ka.com.ua/ua/kak-rabotaet-sovremennyy-smartfon-chto-proiskhodit-v-smartfone-vo-vremya-i-posle-zvonka/ - прототип.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Мобільний комунікаційний пристрій, що містить корпус із розміщеними у ньому технічними засобами, програмним забезпеченням та каналами передачі даних, при цьому до складу програмного забезпечення входить загальне програмне забезпечення і спеціальне програмне забезпечення, причому до складу загального програмного забезпечення входить система захисту, який **відрізняється** тим, що до складу спеціального програмного забезпечення додатково введені система управління мобільним комунікаційним пристроєм, система моніторингу і реагування на кіберінциденти, блок передачі інформації, при цьому до складу системи управління мобільним комунікаційним пристроєм входять підсистема контролю мобільних додатків, підсистема віддаленого налаштування, підсистема шифрування даних і підсистема віддаленого управління, до складу системи моніторингу і реагування на кіберінциденти входять підсистема моніторингу і збору інформації, підсистема аналізу даних, підсистема реагування на кіберінциденти і підсистема оповіщення, причому виходи підсистеми контролю мобільних додатків, підсистеми віддаленого налаштування, підсистеми шифрування даних і підсистеми віддаленого управління, що входять до складу системи управління мобільним комунікаційним пристроєм, з'єднано, відповідно, з першим, другим, третім та четвертим входами блока передачі інформації, вихід підсистеми моніторингу і збору інформації, що входить до складу системи моніторингу і реагування на кіберінциденти, з'єднано послідовно через підсистему аналізу даних і підсистему реагування на кіберінциденти з входом підсистеми оповіщення, вихід якої з'єднано з п'ятим входом блоку передачі інформації, вихід блока передачі інформації з'єднано з входом спеціального програмного забезпечення, а вихід спеціального програмного забезпечення з'єднано каналами передачі даних з автоматизованим робочим місцем адміністратора.



Фіг. 1



Фіг. 2

Комп'ютерна верстка О. Гергіль

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