



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) UA

(11) 101796

(13) C2

(51) МПК

G09C 1/06 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки:	u 2011 06181	(72) Винахідник(и):	Алішов Надір Ісмаїл-огли (UA), Марченко Віталій Анатолійович (UA), Міщенко Олександр Миколайович (UA)
(22) Дата подання заявки:	17.05.2011	(73) Власник(и):	ІНСТИТУТ КІБЕРНЕТИКИ ІМ. В.М. ГЛУШКОВА НАН УКРАЇНИ, вул. Академіка Глушкова, 40, м. Київ-187, 03187 (UA)
(24) Дата, з якої є чинними права на винахід:	25.04.2013	(56) Перелік документів, взятих до уваги експертизою:	UA 92841 C2, 10.12.2010. UA 19899 U, 15.01.2007. RU 2259939 C2, 27.058.2005. RU 2067313 C1, 27.09.1996. RU 2110089 C1, 27.04.1998. RU 2148857 C1, 10.05.2000. RU 2022346 C1, 30.10.1994. SU 1125658 A, 23.11.1984.
(41) Публікація відомостей про заявку:	26.11.2012, Бюл.№ 22		
(46) Публікація відомостей про видачу патенту:	25.04.2013, Бюл.№ 8		

(54) ОБЧИСЛЮВАЛЬНИЙ ПРИСТРІЙ ЗАХИСТУ ІНФОРМАЦІЇ

(57) Реферат:

Винахід належить до систем забезпечення конфіденційності, цілісності й доступності інформаційних ресурсів. Обчислювальний пристрій захисту інформації складається із блока вводу-виводу, блока керування, мікропроцесора, блока генерування випадкових чисел, блока керування пам'яттю, блока асоціативно-функціональної пам'яті, блока оперативного запам'ятовувального пристрою, блока постійного запам'ятовувального пристрою. Винахід додатково містить блок автономного контролю. Перший вхід підключено до четвертого виходу блока керування. Перший вихід підключено до третього входу блока керування. Перший вхід-вихід підключено до четвертого входу-виходу блока керування пам'яттю.

UA 101796 C2

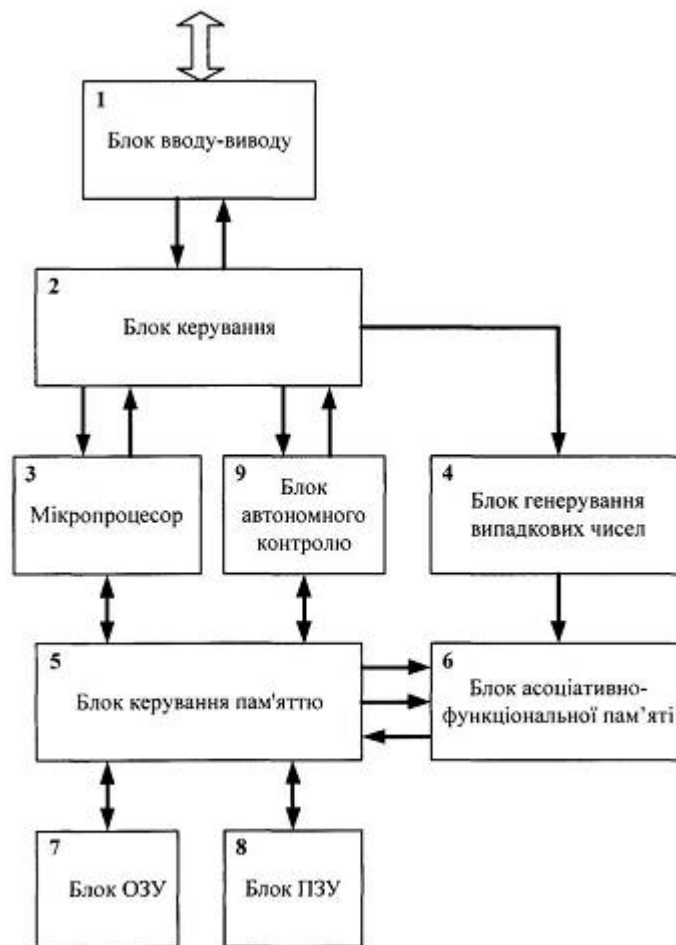


Fig. 2

Винахід належить до області комп'ютерних систем та мереж і може бути використаний при створенні систем забезпечення конфіденційності, цілісності й доступності інформаційних ресурсів.

Відомий пристрій CodeShelter™ (Компанія Software Security Lab, 2005, адреса в Інтернеті www.seculab.ru) який містить блок вводу-виводу, блок керування, мікропроцесор, блок симетричного шифрування, блок генерування випадкових чисел, блок керування пам'яттю, блок оперативного запам'ятовувального пристрою, блок постійного запам'ятовувального пристрою, при цьому перший вхід-вихід блока вводу-виводу є входом-виходом пристрою, другий вхід-вихід підключено до першого входу-виходу блока керування, другий вхід-вихід якого підключений до першого входу-виходу мікропроцесора, четвертий вихід якого підключено до виходу генератора випадкових чисел, третій вихід підключено до виходу блока симетричного шифрування, а другий вхід-вихід підключено до першого входу-виходу блока керування пам'яттю, другий вхід-вихід якого підключений до входу-виходу блока оперативного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу блока постійного запам'ятовувального пристрою.

Загальними ознаками є наявність блока вводу-виводу, блока керування, мікропроцесора, блока керування пам'яттю, блока оперативного запам'ятовувального пристрою, блока постійного запам'ятовувального пристрою, блока генерування випадкових чисел, при цьому перший вхід-вихід блока вводу-виводу є входом-виходом пристрою, другий вхід-вихід підключено до першого входу-виходу блока керування, другий вхід-вихід якого підключено до першого входу-виходу мікропроцесора, другий вихід якого підключено до першого виходу блока керування пам'яттю, другий вхід-вихід якого підключений до входу-виходу блока оперативного запам'ятовувального пристрою, а третій вхід-вихід підключено до входу-виходу блока постійного запам'ятовувального пристрою.

Причиною що заважає досягти технічного результату є те, що пристрій не дозволяє передавати файл будь-якої довжини, щоб при цьому накладні витрати дорівнювали накладним витратам передачі не захищеного файлу, а довжина ключа не впливала на обчислювальну складність що як наслідок не дозволяє забезпечити необхідний рівень захисту від несанкціонованого доступу, формувати шифри, що не розкриваються, файлів і документів.

Відомий пристрій захисту баз даних від копіювання (пат. №19899, Бюл. № 1., опубл. 15.01.2007) який містить блок вводу-виводу, блок керування, мікропроцесор, блок контролю, блок видачі параметрів ключа, блок спеціалізованих обчислень, блок керування пам'яттю, блок оперативного запам'ятовувального пристрою, два блоки постійного запам'ятовувального пристрою, при цьому перший вхід-вихід блока вводу-виводу є входом-виходом системи, другий вхід-вихід підключено до першого входу-виходу блока керування, другий вихід якого підключений до першого виходу мікропроцесора, третій вихід підключений до виходу блока контролю, а четвертий вихід підключений до першого входу-виходу блока видачі параметрів ключа, другий вхід-вихід якого підключений до п'ятого входу-виходу блока керування пам'яттю, четвертий вхід-вихід якого підключений до входу-виходу другого блока постійного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу першого блока постійного запам'ятовувального пристрою, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою, перший вхід-вихід підключено до другого входу-виходу мікропроцесора, третій вхід-вихід якого підключений до входу-виходу блока спеціалізованих обчислень.

Загальними ознаками є наявність блока вводу-виводу, блока керування, мікропроцесора, блока керування пам'яттю, блока постійного запам'ятовувального пристрою, блока оперативного запам'ятовувального пристрою, при цьому перший вхід-вихід блока вводу-виводу є входом-виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора, другий вхід-вихід якого підключено до першого входу-виходу блока керування пам'яттю, другий вхід-вихід якого підключено до входу-виходу блока оперативного запам'ятовувального пристрою, а третій вхід-вихід підключено до входу-виходу блока постійного запам'ятовувального пристрою.

Причиною, що заважає досягненню поставленої задачі є те, що вказаний пристрій не дозволяє забезпечити необхідний рівень захисту від несанкціонованого доступу для розподілених телекомунікаційних систем, організувати протоколи взаємодії з захистом від несанкціонованого модифікування інформації.

Найбільш близьким є обчислювальний пристрій непрямої стеганографії (пат. №92841, Бюл. № 23, опубл. 10.12.2010) який містить блок вводу-виводу, блок керування, мікропроцесор, блок генерації випадкових чисел, блок керування пам'яттю, блок асоціативно-функціональної пам'яті, блок оперативного запам'ятовувального пристрою (ОЗУ), блок постійного запам'ятовувального

пристрою (ПЗУ), при цьому перший вхід-вихід блока вводу-виводу є входом-виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора, а третій вихід підключено до входу блока генерації випадкових чисел, вихід якого підключено до третього входу блока асоціативно-функціональної пам'яті, перший та другий вхід якого підключено до першого та другого виходу блока керування пам'яттю, а перший вихід підключено до першого входу блока керування пам'яттю, перший вхід-вихід якого підключено до другого входу-виходу мікропроцесора, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу постійного запам'ятовувального пристрою.

Загальними ознаками є наявність блока вводу-виводу, блока керування, мікропроцесора, блока генерування випадкових чисел, блока керування пам'яттю, блока асоціативно-функціональної пам'яті, блока оперативного запам'ятовувального пристрою (ОЗУ), блока постійного запам'ятовувального пристрою (ПЗУ), при цьому перший вхід-вихід блока вводу-виводу є входом-виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора, а третій вихід підключено до входу блока генерації випадкових чисел, вихід якого підключено до третього входу блока асоціативно-функціональної пам'яті, перший та другий вхід якого підключено до першого та другого виходу блока керування пам'яттю, а перший вихід підключено до першого входу блока керування пам'яттю, перший вхід-вихід якого підключено до другого входу-виходу мікропроцесора, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу постійного запам'ятовувального пристрою.

Причиною, що заважає досягненню поставленої задачі є те, що вказаний пристрій не дозволяє забезпечити необхідний рівень захисту від несанкціонованого доступу для розподілених телекомунікаційних систем, організувати протоколи взаємодії з захистом від несанкціонованого модифікування інформації.

В основу винаходу поставлено задачу створення такого обчислювального пристрою захисту інформації в комп'ютерних системах та мережах, який при введенні нового блока і зв'язків дозволив реалізувати необхідний рівень захисту для розподілених телекомунікаційних систем, організувати протоколи взаємодії з захистом від несанкціонованого модифікування інформації.

Поставлена задача вирішується тим, що в пристрій, який містить блок вводу-виводу, блок керування, мікропроцесор, блок генерації випадкових чисел, блок керування пам'яттю, блок асоціативно-функціональної пам'яті, блок оперативного запам'ятовувального пристрою (ОЗУ), блок постійного запам'ятовувального пристрою (ПЗУ), при цьому перший вхід-вихід блока вводу-виводу є входом та виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора, а третій вихід підключено до входу блока генерування випадкових чисел, вихід якого підключено до третього входу блока асоціативно-функціональної пам'яті, перший та другий вхід якого підключено до першого та другого виходу блока керування пам'яттю, а перший вихід підключено до першого входу блока керування пам'яттю, перший вхід-вихід якого підключено до другого входу-виходу мікропроцесора, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу постійного запам'ятовувального пристрою, додатково введений блок автономного контролю, причому перший вхід підключено до четвертого виходу блока керування, перший вихід підключено до третього входу блока керування, а перший вхід-вихід підключено до четвертого входу-виходу блока керування пам'яттю.

Відмітними ознаками є наявність блока автономного контролю, причому перший вхід підключено до четвертого виходу блока керування, перший вихід підключено до третього входу блока керування, а перший вхід-вихід підключено до четвертого входу-виходу блока керування пам'яттю. Блок автономного контролю містить вхідний буфер-1, вихідний буфер-1, комутатор, пристрій відображення інформації, пристрій вводу, вхідний-вихідний буфер-2, причому вхід вхідного буфера-1 є першим входом блока, а вихід підключено до першого входу комутатора, перший вихід якого підключено до входу вихідного буфера-1, вихід якого є першим виходом блока, вхід-вихід вхідного-вихідного буфера-2 є першим входом-виходом блока, перший вихід підключено до другого входу комутатора, другий вихід якого підключено до першого входу вхідного-вихідного буфера-2, вихід пристрою вводу підключено до третього входу комутатора, третій вихід якого підключено до входу пристрою відображення інформації.

Введення цього додаткового блока дозволило реалізувати необхідний рівень захисту від несанкціонованого доступу, формувати шифри, що не розкриваються, файлів і документів.

На фіг. 1 представлена блок-схема прототипу.

На фіг. 2 представлена блок-схема запропонованого пристрою.

На фіг. 3 представлена блок-схема блока керування.

На фіг. 4 представлена блок-схема блока керування пам'яттю.

5 На фіг. 5 представлена блок-схема блока автономного контролю.

На фіг. 6 представлена блок-схема блока асоціативно-функціональної пам'яті.

Запропонований обчислювальний пристрій захисту інформації (фіг. 2) містить блок вводу-виводу 1, блок керування 2, мікропроцесор 3, блок генерування випадкових чисел 4, блок керування пам'яттю 5, блок асоціативно-функціональної пам'яті 6, блок оперативного
10 запам'ятовувального пристрою 7 (ОЗУ), блок постійного запам'ятовувального пристрою 8 (ПЗУ), блок автономного контролю 9, при цьому перший вхід-вихід блока вводу-виводу 1 є входом та виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування 2, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора 3, а третій вихід підключено до входу блока генерування випадкових чисел 4, вихід якого
15 підключено до третього входу блока асоціативно-функціональної пам'яті 6, перший та другий вхід якого підключено до першого та другого виходу блока керування пам'яттю 5, а перший вихід підключено до першого входу блока керування пам'яттю 5, перший вхід-вихід якого підключено до другого входу-виходу мікропроцесора 3, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою 7, третій вхід-вихід підключено до
20 входу-виходу постійного запам'ятовувального пристрою 8, а четвертий вхід-вихід підключено до першого входу-виходу блока автономного контролю 9, перший вхід якого підключено до четвертого виходу блока керування, а перший вихід підключено до третього входу блока керування.

Як мікропроцесор 3 може бути використаний процесор Pentium III (компанія Intel, www.intel.com), блок керування пам'яттю 5 реалізується на стандартному чипсеті Intel 840 (компанія Intel, www.intel.com).

Блок керування 2 представлений на фіг. 3 і складається із трьох вхідних буферів 10, 14, 16, чотирьох вихідних буферів 11, 13, 15, 17, комутатора 12, при чому вхід вхідного буфера-1 10 є першим входом блока керування, вихід якого підключено до першого входу комутатора 12,
30 перший вихід якого підключено до входу вихідного буфера-1 11, вихід якого є першим виходом блока керування, вхід вхідного буфера-2 14 є другим входом блока керування, вихід якого підключено до другого входу комутатора 12, другий вихід якого підключено до входу другого вихідного буфера-2 13, вихід якого є другим виходом блока керування, третій вихід комутатора 12 підключений до входу вихідного буфера-3 17 вихід якого є третім виходом блока, вхід вхідного буфера-3 16 є третім входом блока керування, вихід якого підключено до третього входу комутатора 12, четвертий вихід якого підключено до входу четвертого вихідного буфера-4
35 15, вихід якого є четвертим виходом блока керування.

Блок керування пам'яттю 5 представлений на фіг. 4 і складається із семи регістрів 18, 19, 20, 21, 23, 24, 25 та пристрою керування 22, причому перший вхід-вихід регістра 18 є першим входом-виходом блока, а другий вхід-вихід підключено до першого входу-виходу пристрою керування 22, другий вхід-вихід якого підключено до першого входу-виходу регістра 19, другий вхід-вихід якого є другим входом-виходом блока, третій вхід-вихід пристрою керування 22 підключено до першого входу-виходу регістра 20, другий вхід-вихід якого є третім входом-виходом блока, четвертий вхід-вихід пристрою керування 22 підключено до першого входу-виходу регістра 21, другий вхід-вихід якого є четвертим входом-виходом блока, перший вихід пристрою керування 22 підключено до входу регістра 23 вихід якого є першим виходом блока, другий вихід пристрою керування 22 підключено до входу регістра 24 вихід якого є другим виходом блока, перший вхід пристрою керування 22 підключено до виходу регістра 25 вхід якого є першим входом блока.

Блок автономного контролю 9 представлений на фіг. 5 і складається із вхідного буфера 26, вихідного буфера 27, комутатора 28, пристрою відображення інформації 29, пристрою вводу 30, вхідного-вихідного буфера-2 31, причому вхід вхідного буфера-1 26 є першим входом блока, а вихід підключено до першого входу комутатора 28, перший вихід якого підключено до входу вихідного буфера-1 27, вихід якого є першим виходом блока, вхід-вихід вхідного-вихідного
55 буфера-2 31 є першим входом-виходом блока, перший вихід підключено до другого входу комутатора 28, другий вихід якого підключено до першого входу вхідного-вихідного буфера-2 31, вихід пристрою вводу 30 підключено до третього входу комутатора 28, третій вихід якого підключено до входу пристрою відображення інформації 29.

Блок асоціативно-функціональної пам'яті 6 представлений на фіг. 6 і складається із регістра адрес лівий 32, регістра адрес правий 33, асоціативної пам'яті лівої 34, асоціативної пам'яті

правої 35, регістра даних лівий 36, регістра даних правий 37, причому вхід регістра даних лівий. 32 є першим входом блока, вхід-вихід якого підключено до входу-виходу блока асоціативна пам'ять ліва 34, вхід якого підключено до виходу регістра даних лівий 36, вхід якого є третім входом блока, а другий вихід підключено до входу регістра адрес правий 33, вхід якого є другим входом блока, а вихід підключено до входу блока асоціативна пам'ять права 35, вхід-вихід якого підключено до входу-виходу регістра даних правий 37, перший вихід якого є виходом блока, а вхід підключено до виходу регістра адрес лівий 32.

Пристрій функціонує наступним чином. На першому етапі роботи пристрою, що називається Початкове налаштування, по команді із блока керування 2 включається робота блока генерації випадкових чисел 4: що генерує двійкові послідовності байтів. Вихідні послідовності байтів надходять до блока асоціативно-функціональної пам'яті 6 у регістр даних лівий 36. Адреси записуваних байтів для блока асоціативна пам'ять ліва 34 формуються блоком керування пам'яттю 5. Ці адреси одночасно передаються в регістр даних правий 37, а вміст регістра даних лівий 36 передається, як адреси, для блока асоціативна пам'ять права 35, у регістр адрес правий 33. При цьому коректність формування, як адресної частини, так і даних для блока асоціативна пам'ять ліва 34 і блока асоціативна пам'ять права 35 контролюється блоком керування пам'яттю 5 керованого від мікропроцесора 3. Початкова установка завершується після формування відповідних масивів даних в блоці асоціативна пам'ять ліва 34 та блоці асоціативна пам'ять права 35. Після завершення цього етапу пристрій вважається готовим до роботи й може проводити шифрування й дешифрування даних.

Далі для аутентифікації користувача він повинен ввести правильні ідентифікаційні дані за допомогою пристрою вводу 30, які зашифровуються та відправляються адресату на перевірку. В разі успішного проходження перевірки пристрій вважається готовим до роботи.

Для організації захищеної транзакції, масив даних що підлягає захисту надходить від блока вводу-виводу 1 через блок керування 2 та мікропроцесор 3, за допомогою блока керування пам'яттю 5 у блок ОЗУ 7 окремими порціями.

З початкового масиву даних виділяється набір полів які були раніше вказані користувачем для перевірки та пересилаються з ОЗУ 7 через блок керування пам'яттю 5 в блок автономного контролю. В блоці автономного контролю 9 отримані дані з вхідного-вихідного буфера-2 31 через комутатор 28 виводяться на пристрій відображення інформації 29. Для підтвердження коректності даних користувач порівнює відображувані дані на пристрою відображення інформації 29 з початковими даними що були відправлені на пристрій захисту з головного комп'ютера. Якщо дані співпадають то користувач використовуючи пристрій вводу 30 підтверджує коректність та дозволяє подальше проведення поточної операції якщо операція не підтверджується то подальша обробка даних припиняється.

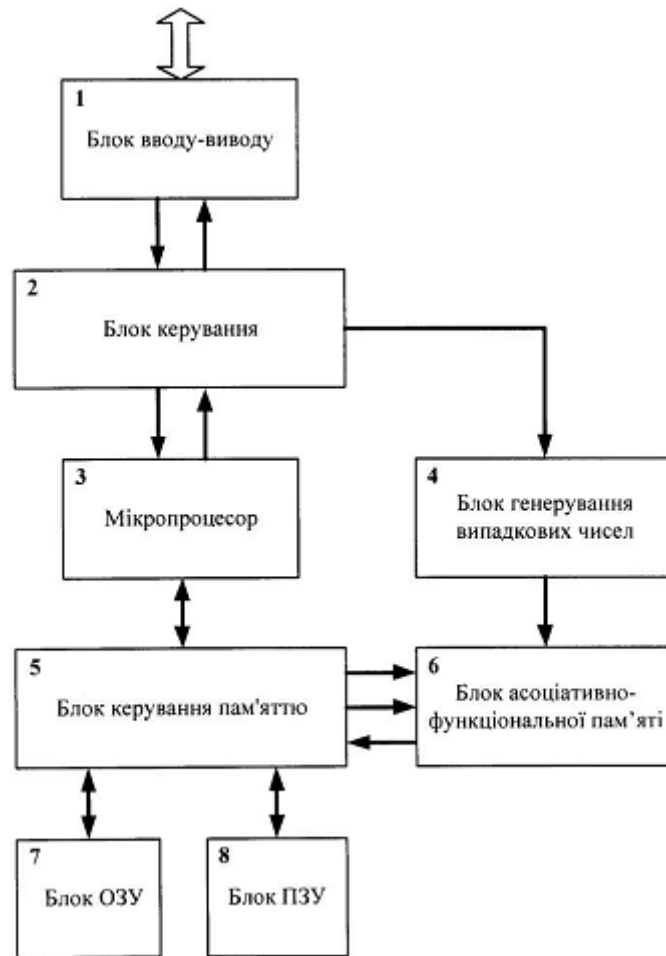
В разі успішного підтвердження поточної операції записана в ОЗУ 7 порція інформації побайтно передається в блок асоціативно-функціональної пам'яті 6 через блок керування пам'яттю 5 та регістр адрес правий 33 у блок асоціативна пам'ять права 35, як адресна інформація. У регістрі даних правий 37 блока асоціативно-функціональної пам'яті 6 формується байт, що є вмістом елемента блока асоціативна пам'ять права 35 розміщеним за адресою записаною в регістр адрес правий 33. Цей байт заміщає відповідний байт в ОЗУ 7. Цей процес повторюється поки у вихідному масиві, що шифрується, не буде повністю заміщені всі байти з блока асоціативна пам'ять права 35. Шифрований файл через блок вводу-виводу 1 передається в головний комп'ютер.

При дешифруванні, масив даних, що підлягає дешифруванню, через блок вводу-виводу 1 записується порціями через блок керування 2 та мікропроцесор 3, за допомогою блока керування пам'яттю 5 у блок ОЗУ 7. Далі записана в ОЗУ 7 порція інформації побайтно передається через блок керування пам'яттю 5 у блок асоціативно-функціональної пам'яті 6 за допомогою регістра адрес лівий 32 до асоціативної пам'яті лівої 34 як адресної інформації. У регістрі даних лівий 36 формується байт, що є вмістом елемента за адресою, записаному в регістрі адрес лівий 32. Цей процес повторюється поки у вихідному дешифрованому масиві не буде повністю заміщені всі байти з блока асоціативна пам'ять ліва 34. Дешифрований файл через блок вводу-виводу 1 передається в головний комп'ютер.

Обчислювальний пристрій захисту інформації, як виходить з опису, може бути реалізований промисловим чином, тому що складові блоки можуть бути побудовані на основі елементної бази широкого застосування.

ФОРМУЛА ВИНАХОДУ

1. Обчислювальний пристрій захисту інформації, що складається із блока вводу-виводу, блока керування, мікропроцесора, блока генерування випадкових чисел, блока керування пам'яттю, блока асоціативно-функціональної пам'яті, блока оперативного запам'ятовувального пристрою, блока постійного запам'ятовувального пристрою, при цьому перший вхід-вихід блока вводу-виводу є входом та виходом пристрою, другий вхід та вихід підключено до першого входу та виходу блока керування, другий вхід та вихід якого підключено до першого входу та виходу мікропроцесора, а третій вихід підключено до входу блока генерування випадкових чисел, вихід якого підключено до третього входу блока асоціативно-функціональної пам'яті, перший та другий вхід якого підключено до першого та другого виходу блока керування пам'яттю, а перший вихід підключено до першого входу блока керування пам'яттю, перший вхід-вихід якого підключено до другого входу-виходу мікропроцесора, другий вхід-вихід підключено до входу-виходу блока оперативного запам'ятовувального пристрою, третій вхід-вихід підключено до входу-виходу постійного запам'ятовувального пристрою, який **відрізняється** тим, що додатково містить блок автономного контролю, причому перший вхід підключено до четвертого виходу блока керування, перший вихід підключено до третього входу блока керування, а перший вхід-вихід підключено до четвертого входу-виходу блока керування пам'яттю.
2. Обчислювальний пристрій за п. 1, який **відрізняється** тим, що блок автономного контролю містить вхідний буфер-1, вихідний буфер-1, комутатор, пристрій відображення інформації, пристрій вводу, вхідний-вихідний буфер-2, причому вхід вхідного буфера-1 є першим входом блока, а вихід підключено до першого входу комутатора, перший вихід якого підключено до входу вихідного буфера-1, вихід якого є першим виходом блока, вхід-вихід вхідного-вихідного буфера-2 є першим входом-виходом блока, перший вихід підключено до другого входу комутатора, другий вихід якого підключено до першого входу вхідного-вихідного буфера-2, вихід пристрою вводу підключено до третього входу комутатора, третій вихід якого підключено до входу пристрою відображення інформації.



Фіг. 1

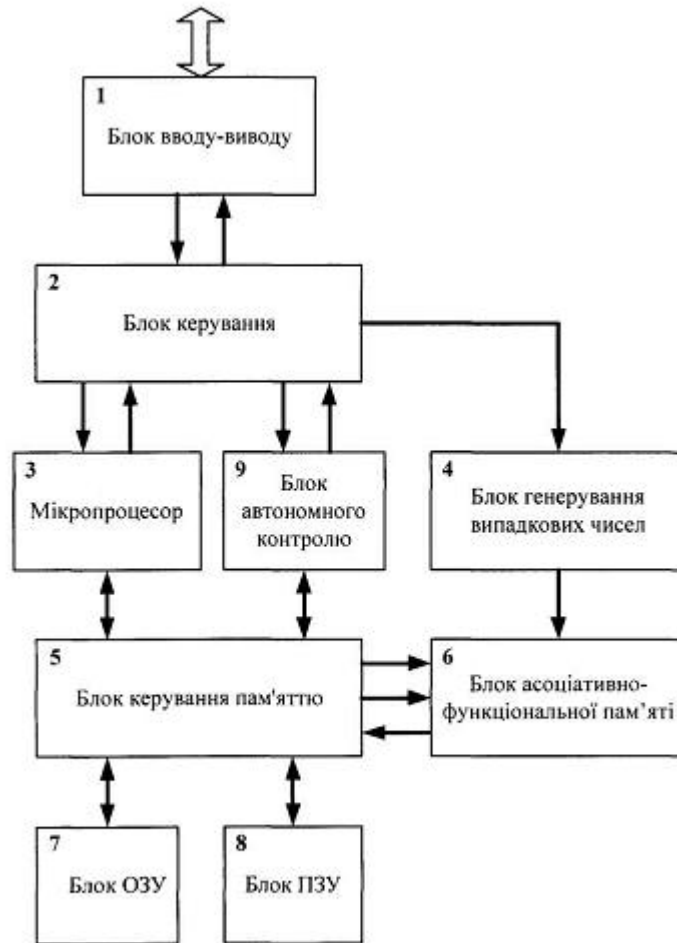


Fig. 2

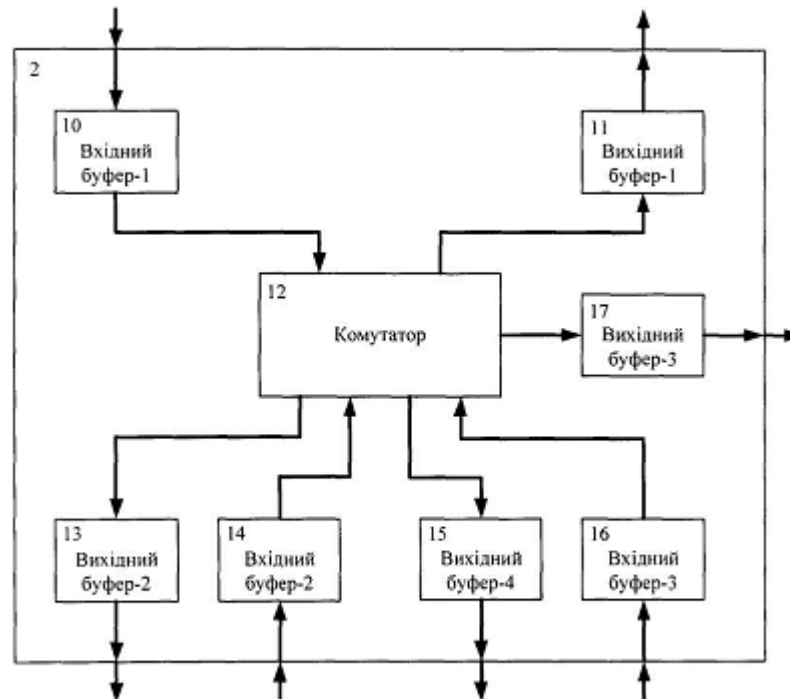
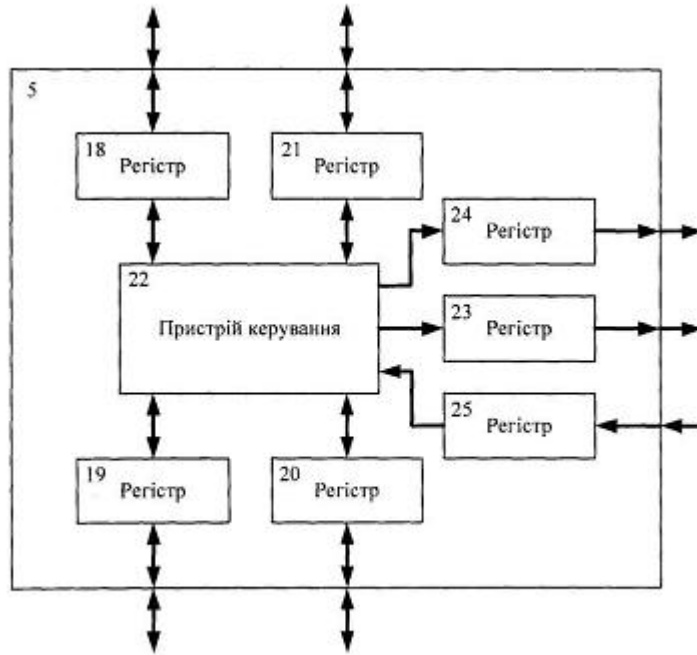
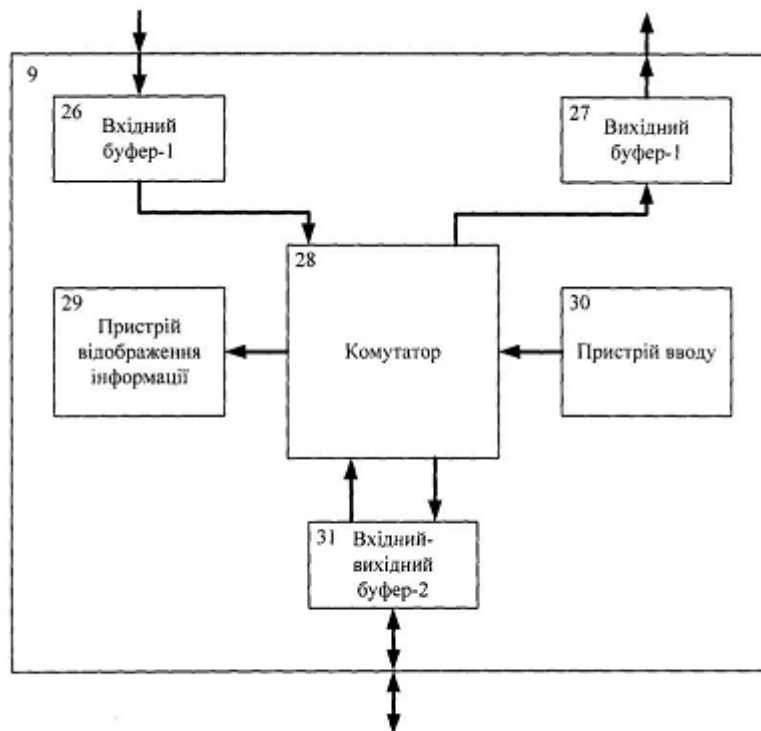


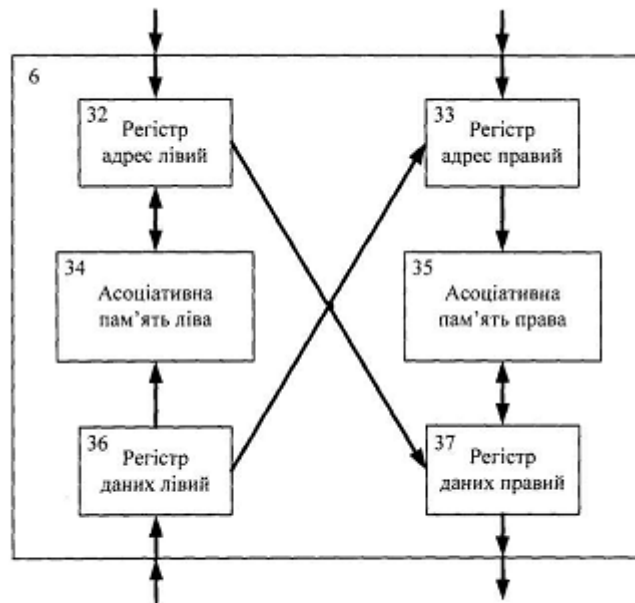
Fig. 3



Фіг. 4



Фіг. 5



Фіг. 6

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