УДК 681.325.5-181.4

ГАРАНТОЗДАТНА СИСТЕМА ОБРОБЛЕННЯ НАВІГАЦІЙНИХ І КАРТОГРАФІЧНИХ ДАНИХ

А. Бондарук, В. Глухов*, К. Євтушенко, Н. Заіченко, В. Калінічев, Б. Оліярник
*Львівський науково-дослідний радіотехнічний інститут, * Національний університет «Львівська політехніка»*

Анотація: **Формулюється підхід до проектування гарантоздатної системи оброблення навігаційних та картографічних даних, що пропонується для використання в автоматизованих системах керування взаємодією об'єктів бронетанкової техніки і ракетно-артилерійських систем.**
Summary: **In this article dependable computer navigation and cartographical information processing system for armoured vehicles and artillery team-work ACS is discussed.**
Ключові слова: **Гарантоздатні комп'ютерні системи, навігаційні дані, картографічні дані.**

Вступ

Ефективність використання об'єктів бронетехніки на полі бою в значній мірі залежить від ступеня інформаційної переваги над противником. Це досягається використанням автоматизованих систем керування на базі спеціалізованих ЕОМ. Зберігання, оброблення та передавання інформації в таких системах пов'язані з ризиками втрати, розкриття, модифікації, підміни, нав'язування в результаті дій противника, легального абонента під час передавання даних відкритими каналами зв'язку. Тому обов'язковою вимогою до таких систем є їхня гарантоздатність, складовою частиною якої є конфіденційність. Особливості поєднання комп'ютерних систем для оброблення навігаційних та картографічних даних і гарантоздатних (конфіденційних) комп'ютерних систем в літературі описані недостатньо. У роботі пропонується метод проектування таких систем, який ґрунтується на використанні шифропроцесора, що працює відповідно до діючих в Україні стандартів, у тому числі і стандарту на цифровий підпис з використанням еліптичних кривих.

І Аналіз публікацій і окреслення проблеми

Від комп'ютерних засобів систем керування завжди, крім вирішення основного завдання керування, вимагалося задоволення вимоги надійності. Термін «надійність» в його сучасному розумінні набуває відтінку «довірчості». Концепція довірчої надійності практично збігається з тим, що прийнято називати dependability (гарантоздатність, яка забезпечує отримання достовірних результатів за наявності несправностей). Визначення гарантоздатності міститься в міжнародних стандартах [1, 2]. Більш вузько визначають поняття гарантоздатності військові документи [3, 4].

Для забезпечення конфіденційності, цілісності та достовірності інформації вживаються організаційні та технічні заходи [5 – 7], які реалізуються апаратно-програмними засобами. Проте, якщо в системі наявні лише відкриті канали обміну інформацією, питання забезпечення криптостійкості та імітостійкості залишаються не в достатній мірі вирішеними.

У той же час відомі криптографічні методи забезпечення гарантоздатності, які базуються на використанні шифропроцесорів. Одним з методів забезпечення конфіденційності гарантоздатних систем є використання електронного цифрового підпису на основі еліптичних кривих. В Україні діють два стандарти на цифровий підпис [8, 9]. Також стандартизовані і процедури шифрування і гешування [10, 11]. У [12, 13] представлена багаторівнева структура шифропроцесора, який здійснює криптографічні перетворення відповідно до стандартів [8 – 11]. Для практичної реалізації шифропроцесора корисними є рекомендації та вимоги міжнародного стандарту IEEE 1363-2000 [14].

Львівський науково-дослідний радіотехнічний інститут упродовж десятиліть здійснює розроблення і впровадження бортових інформаційно-керуючих систем для бронетанкової техніки [15, 16]. Логічним розширенням таких робіт була робота зі створення апаратної основи для побудови бортових автоматизованих систем керування взаємодією, в тому числі і шифропроцесорів [12, 13].

Хоча особливості проектування комп'ютерних систем [17], систем для оброблення навігаційних [18] та картографічних [19] даних і гарантоздатних комп'ютерних систем, в тому числі криптографічних систем [20, 12, 13], добре відомі, особливості поєднання таких систем в літературі описані недостатньо.

У даній роботі розглядається питання розроблення багаторівневої структури шифропроцесора, що входить до складу комп'ютерних систем оброблення навігаційних та картографічних даних і забезпечує їхню

конфіденційність – один з основних елементів гарантоздатності. Пропонована структура використовує підходи багаторівневої моделі відкритих систем і реалізує сучасні математичні методи криптографії.

II Цілі статті

Метою роботи є узагальнення принципів проектування гарантоздатних систем оброблення навігаційних та картографічних даних. У системі використовуються відкриті канали зв'язку, а підвищення рівня захисту даних досягається застосуванням криптографічних методів.

У роботі пропонується метод проектування багаторівневої структури шифропроцесора, що входить до складу гарантоздатних систем оброблення навігаційних та картографічних даних і забезпечує їхню конфіденційність, цілісність та достовірність.

III Структура гарантоздатної системи

Згідно з [3] гарантоздатність визначає міру здатності об'єкта бути працездатним і виконувати покладені на нього функції у будь-який час виконання покладеної на нього місії за умови, що на початку виконання місії об'єкт був придатний до виконання цих функцій.

Система гарантоздатна, коли вона доступна, надійна, безпечна, захищена (здатна зберегти конфіденційність, забезпечувати цілісність), ремонтопридатна.

Кожний об'єкт гарантоздатної системи, а також центр розповсюдження картографічної інформації можна представити у вигляді дворівневої системи (рис. 1) – бортова ЕОМ і шифропроцесор (ШП). Шифропроцесор є засобом протистояння діям ворожого оточення. У пропонованій системі на нього покладаються завдання криптографічного захисту та верифікації інформації.

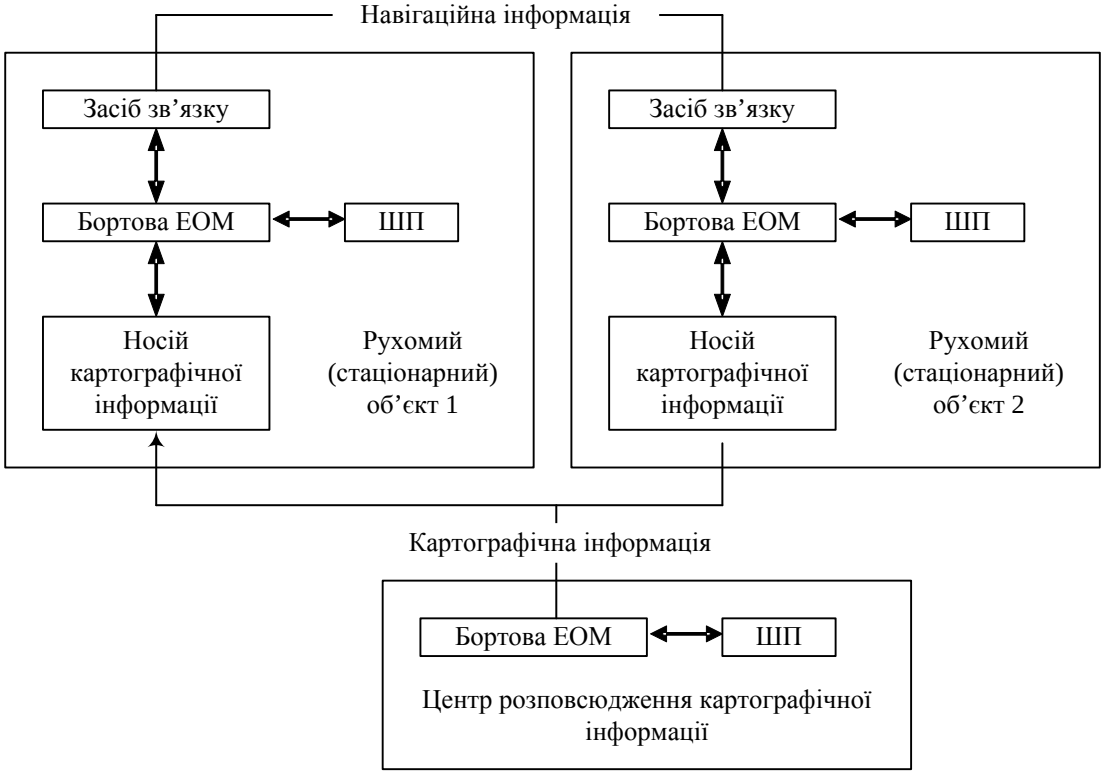

Рисунок 1 – Структура системи (варіант)

IV Структура шифропроцесора

Для побудови шифропроцесора використовується центральний процесор і криптографічний спецпроцесор (або декілька спецпроцесорів), при цьому спецпроцесори можуть бути виконані у вигляді ядер надвеликої інтегральної схеми (НВІС) [21]. Актуальним є завдання організації ефективної взаємодії центрального і спецпроцесорів, а також завдання вибору системи команд останнього.

Відомі декілька методів взаємодії центрального процесора і спеціалізованого. Центральний процесор може сприймати спецпроцесор як: 1) сопроцесор; 2) набір портів; 3) канал [22, 23].

Перший метод вимагає глибокого знання особливостей архітектури центрального процесора, його системи команд, використання її кодів для запуску сопроцесора. До того ж даний метод вимагає апаратної підтримки з боку центрального процесора. Другий і третій методи позбавлені цих недоліків.

Представлення спецпроцесора як канала дає можливість використати еталонну модель взаємодії відкритих систем [17] для розподілення функцій між елементами системи. Взаємодія між бортовою ЕОМ і шифропроцесором відбувається на протокольному (найвищому) рівні. Потік інформації під час її оброблення в шифропроцесорі спочатку опускається з верхнього рівня на найнижчий, а потім знову підіймається на верхній (наприклад, під час шифрування відкрита інформація опускається з верхнього рівня на найнижчій, а потім зашифрована інформація підіймається з найнижчого рівня на найвищий – рис. 2).

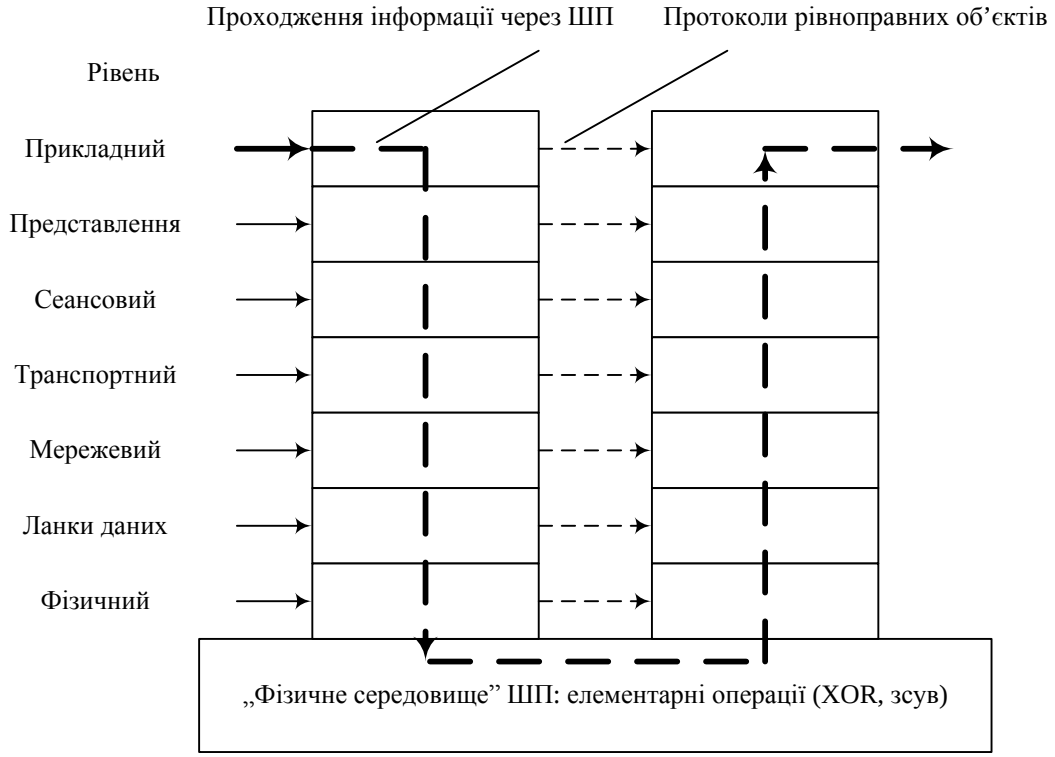

Рисунок 2 – Структура шифропроцесора

Кожний N-рівень шифропроцесора є N-спецпроцесором, який складається з протокольного N-процесора і (N–1)-спецпроцесора.

Стандарти, що діють в України, повністю визначають алгоритми роботи всіх спецпроцесорів. Міжнародні стандарти [14] є цінним і корисним доповненням до вітчизняних стандартів.

Усі спецпроцесори мають аналогічну структуру (рис. 3).

Рисунок 3 – Структура N-спецпроцесора

Універсальний N-процесор реалізується як процесор із скороченою системою команд (RISC).

Розподіл завдань між різними рівнями шифропроцесора, що обробляє електронні підписи, ілюструє таблиця 1. Розподіл завдань між рівнями дає можливість визначити систему команд кожного зі спеціалізованих процесорів.

Таблиця 1 - Розподіл задач між різними рівнями шифропроцесора (рівні представлення – згідно з [14])

Рівень шифропроцесора	Рівень представлення	Тип операцій	Операції
1 (найнижчий)	Примітиви	Операції над елементами поля Галуа в нормальній формі	Піднесення до квадрату, визначення розрядів добутку
2	Примітиви	Операції над елементами поля Галуа в нормальній та поліноміальній формах	Множення, додавання, пересилання
3	Схеми	Операції над точками еліптичних кривих, криптографічні перетворення	Додавання, подвоєння, множення на число

V Метод проектування гарантоздатних комп'ютерних систем (у частині забезпечення конфіденційності)

Узагальнений метод проектування гарантоздатних комп'ютерних систем (у частині забезпечення конфіденційності) складається з послідовності проектних рішень:

система представляється як сукупність апаратно-програмних засобів, що виконують основне завдання, і апаратно-програмних засобів забезпечення конфіденційності (шифропроцесор);

шифропроцесор є багаторівневою структурою відповідно до еталонної моделі взаємодії відкритих систем;

кожний N-рівень шифропроцесора є N-спецпроцесором, який складається з протокольного N-процесора і (N–1)-спецпроцесора;

кожний універсальний N-процесор реалізується як процесор із скороченою системою команд (RISC);

продуктивність та інтерфейси універсального процесора визначаються особливістю системи оброблення навігаційних та картографічних даних;

кожний із спецпроцесорів реалізує одне з завдань (або декілька завдань, або частину завдань) забезпечення конфіденційності;

кожний із спецпроцесорів працює відповідно до національного стандарту;

система команд спецпроцесора визначається алгоритмом вирішення відповідного завдання;

кількість спецпроцесорів визначається обсягом навігаційних та картографічних даних та заданим часом їхнього опрацювання;

процесори реалізуються у вигляді ядер НВІС (практично – ПЛІС), утворюючи так звану «систему на кристалі».

Даний підхід дозволяє створити модульну ієрархічну структуру, до якої застосовуються методи паралельного і одночасного проектування, виготовлення, налагодження і тестування.

Висновки

Викладено та проілюстровано метод проектування гарантоздатних систем оброблення навігаційної та картографічної інформації, який поєднує відомі принципи побудови систем оброблення навігаційної та картографічної інформації з принципами, що забезпечують її конфіденційність, цілісність, достовірність, а також імітостійкість та криптостійкість системи. Метод реалізований у розробках Львівського науково-дослідного радіотехнічного інституту.

Подальший розвиток методу полягає у збільшенні номенклатури спецпроцесорів для забезпечення роботи відповідно до стандартів інших країн та міжнародних організацій, для оптимізації продуктивності та апаратних витрат, а також у збільшенні номенклатури інтерфейсів для під'єднання шифропроцесора до перспективних комп'ютерних систем.

Література: ***1.*** *IEC 50(191):1990 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 135 p.* ***2.*** *IEC 60050-191-am2 (2002) Ed. 1.0 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service.* ***3.*** *Military handbook MIL-HDBK-338b. Electronic reliability design handbook. Department of defense of USA. 1 october 1998.* ***4.*** *AFSC-TR-65-6, Chairman's Final Report. Weapon System Effectiveness Industry Advisory Committee (WSEIAC), Air Force Systems Command, January 1965, (AD-467816).* ***5.*** *Петров А. А. Компьютерная безопасность. Криптографические методы. - М.: ДМК Пресс, 2000. - 448 с. ил.* ***6.*** *ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования".* ***7.*** *Программы для предотвращения*

несанкционированного доступа к информации. КомпьютерПресс №3'2008. ***8.*** *Межгосударственный стандарт ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997.* ***8.*** *ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ. Державний комітет України з питань технічного регулювання та споживчої політики. 2003.* ***10.*** *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Государственный комитет СССР по стандартам. Москва. 1989.* ***11.*** *Межгосударственный стандарт ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хеширования. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997.* ***12.*** *В. Глухов, Н. Заіченко, Б. Оліярник. Шифропроцесор для бортових інформаційно-керуючих систем. Наукові нотатки. Міжвузівський збірник (за напрямком «Інженерна механіка»), випуск 19 (січень 2007). Луцький державний технічний університет, Луцьк. 2007. С.33-43.* ***13.*** *В. С. Глухов, К. С. Євтушенко, Н. В. Заіченко, Б. О. Оліярник "Криптографічні засоби спеціалізованої бортової ЕОМ для бронетехніки" 7 с. Вісник Хмельницького національного університету №2, 2007. Технічні науки. Том 2. с.29-33. Хмельницький, 2007.* ***14.*** *IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000.* ***9.*** *В. С. Глухов, Н. В. Заіченко, Б. О. Оліярник, А. Б. Бондарук. Особливості проектування обчислювальних модулів для бортових інформаційно-керуючих систем бронетанкової техніки. "Механіка та машинобудування" // Науково-технічний журнал – Харків: НТУ «ХПІ», 2006. - №1, -311 с. С.238-244.* ***10.*** *Глухов В. С., Заіченко Н. В., Іванов В. І., Оліярник Б. О., Тупиця А. В. Обчислювальні модулі для бортових інформаційно-керуючих систем бронетанкової техніки. "Механіка та машинобудування". Науково-технічний журнал N1'2000. Харківський державний політехнічний університет, Відділення механіки та машинобудування Академії наук Вищої школи України. Харків, 2000.* ***17.*** *ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Базова модель (ISO/IEC 7498-1:1994, IDT).* ***18.*** *Автомобильная навигационная система POCKET GPS PRO MOSCOW. http://www.sysnavigation.ru/articles/1818/* ***19.*** *Электронная картографическая навигационная информационная система SAVENAV-3. http://www.ntutc.ru/kartografia.htm* ***20.*** *В.С. Глухов. Система команд криптографічного процесора " // Вісник Національного університету "Львівська політехніка" № 523 «Комп'ютерні системи та мережі». Львів. Видавництво Національного університету «Львівська політехніка». 2004. С.42 – 50.* ***21.*** *А. О. Мельник, Т. А. Коркішко. Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів // Вісник Державного університету "Львівська політехніка" № 385 «Комп'ютерні системи та мережі». Львів. Видавництво Державного університету «Львівська політехніка». 2000. С. 77 – 80.* ***22.*** *В. Б. Аронов, В. С. Глухов, Я. К. Деревенко, Н. В. Заиченко, С. Ф. Федуняк. Одноплатный арифметический процессор, подключаемый к магистрали ГОСТ 26765.51-86, и средства обеспечения его серийного производства // "1-ая научно-техническая конференция НПО "Фазотрон". Тезисы докладов. Москва, 19-21 сентября 1989 г.* ***23.*** *В. С. Глухов, Н. В. Заиченко. Арифметический спецвычислитель с кэш-памятью команд. "Тезисы докладов 29-ой научно-технической конференции НПО "Антей". Москва, 1990 г*

УДК 004.056.5:004.057.2(045)

КРИПТОГРАФИЧЕСКИЕ ОСНОВАНИЯ РАЗРАБОТКИ СТАНДАРТА СТ РК 1073-2007

Альжан Абдрахманов, Дана Байбатчаева
КНБ Республики Казахстан

Аннотация: **Рассматривается концепция построения стандарта СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования", общие требования к средствам криптографической защиты информации (СКЗИ), основания выбора допустимых диапазонов значений основных параметров криптографических алгоритмов, дополнительные меры безопасности.**

Summary: **Constructing conception of the standard ST RK 1073-2007 "Means of cryptographic information protection. General technical requirements", general requirements for MCIP, reasons of the selection of**