ЗАХИСТ ІНФОРМАЦІЇ

УДК 004:623

В.П. Данилович, кандидат фізико-математичних наук, професор,
М.О. Живко, ад'юнкт кафедри ОРД ЛДУВС,
В.Д. Смичок, кандидат технічних наук

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ДОДАТКОВИХ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У статті розглянуто особливості використання додаткових технічних засобів захисту інформації в аспекті протидії злочинності у процесі діяльності правоохоронних органів. Запропоновано впровадити у виробництво спеціальний шифрувальний пристрій як спецзасіб оперативних підрозділів органів внутрішніх справ.

Ключові слова: *аналог, динаміка, інформація, захист інформації, код, мережа, нелінійна локація, оперативно-розшукова діяльність, телефон, функція, шифрування.*

В статье рассмотрены особенности использования дополнительных технических средств защиты информации в аспектах противодействия преступности в процессе деятельности правоохранительных органов. Предлагается внедрить в производство специальное шифровальное устройство как спецсредство оперативных подразделений органов внутренних дел.

Ключевые слова: *аналог, динамика, информация, защита информации, код, сеть, нелинейная локация, оперативно-розыскная деятельность, телефон, функция, шифрование.*

Features of use of the additional means of an information security from the aspects of counteraction to criminality in the course of law enforcement bodies' activities are considered. It is offered to introduce into an industry special cryptographic hardware as a special device for operative divisions of law-enforcement bodies.

Keywords: *analog, dynamics, information, information security, code, network, nonlinear location, operational and investigative activities, phone, function, encryption.*

Світові процеси глобалізації, впровадження новітніх інформаційних технологій, формування інформаційного суспільства посилюють важливість такої складової національної безпеки, як інформаційна безпека, а відтак і захист інформації. Важлива роль захисту інформації випливає з розуміння того, що захист інформації є не тільки однією з головних складових національної безпеки держави, але й невід'ємною компонентною усіх інших її складових; інформаційні стратегії в сучасних умовах набувають важливого значення під час реалізації різних моделей співробітництва, захисту населення та дотримання законності або відіграють роль своєрідної "інформаційної зброї"; руйнування та дезорганізація інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення; витік інформації в процесі діяльності

органів внутрішніх справ призводить до зростання злочинності, її безкарності та зневіри населення тощо. Інформація повинна бути захищеною як правовими актами, так і технічними засобами. Існує низка сучасних технічних засобів, що використовуються у практичній діяльності правоохоронних органів, а зокрема, оперативних підрозділів, для захисту інформаційних ресурсів. Ми пропонуємо розглянути та впровадити у діяльність ОВС один із засобів захисту інформації, що слугує для захисту інформації в процесі проведення оперативно-розшукової діяльності.

Детальну інформацію про методи шифрування та захист інформації можна знайти [1, 2, 3], починаючи від шифрів Юлія Цезаря "частокіл-16" і закінчуючи німецькою арифметичною шифрувальною машиною "Венігда" та криптографічними протоколами Алана Тюрінга [2]. З розвитком технологій шифрувальна техніка та криптографічні алгоритми значно вдосконалились. Криптографія на сучасному рівні об'єднує знання в галузі обчислювальної техніки, теорії інформації, теорії штучного інтелекту та ін. [6]. Нині існує велика кількість комп'ютерних технологій та алгоритмів, на основі яких створено відповідне програмне забезпечення захисту інформації. Довжина ключа може тривати від долі секунди до декількох місяців зі швидкістю у мільярди операцій за секунду залежно від ступеня таємності або актуальності інформації. Незважаючи на це, вторгнення в інформаційні, а особливо наукоємні комп'ютерні системи, є основною проблемою кодування і декодування інформації. Щоб надійно захистити джерело інформації, крім чисто фізичного розриву (відключення комп'ютера від різного роду мережевих з'єднань), використовують обов'язкове екранування електромагнітного випромінювання шифрувального обладнання. Різноманітні способи екранування дають позитивний ефект при спробі вторгнення в носій інформації методом локаційного радіоперехоплення. Проблемою є те, що усі ці заходи безпеки відпрацьовані вже багато років, але існує декілька способів їх "зламати", що в залежності від кваліфікації криптографіста можуть бути використані будь-якою зацікавленою стороною [3].

Захист інформації важлива проблема в умовах інформаційного суспільства, щоб ідею впровадження технічних заходів вважати достатньо ефективною. Проблемою технічних засобів захисту інформації у свій час займались Ю. Максимов, В. Сонніков, В. Петров, А. Паршуткін, М. Єремєєв, а з українських вчених на цей час: Ю. Добуш, О. Рибальський, І. Горбенко, В. Захаров, Г. Гулак, В. Хорошко, Ю. Орлов, О. Потій, Ю. Горбунко та інші.

Законодавча база України з питань захисту інформації в інформаційній сфері впродовж останніх років поповнилася наступними законами: "Про інформацію" [7], "Про державну таємницю" [8], "Про захист інформації в автоматизованих системах" [9], "Про науково-технічну інформацію" [10], "Про Службу безпеки України" [11], "Про міліцію" [12] тощо. Однак наше законодавство не встигає за розвитком новітніх технологій, особливо пов'язаних з розвитком комп'ютерної техніки. Тому питання правового регулювання боротьби з комп'ютерною злочинністю на сьогодні стоїть дуже гостро. Кіберзлочинці настільки вміло та професійно використовують досягнення НТП, що навіть професіонали із захисту інформації державних структур, не говорячи про правоохоронців, які не є спеціалістами з комп'ютерної техніки, з труднощами вирішують поставлені завдання.

Ст. 11 Закону України про міліцію в пункті "Пошукові заходи", "Розвідувальні заходи" та "Контррозвідувальні заходи" передбачає застосування спеціальних засобів і методів у практиці оперативно-розшукової діяльності [12, 16]. У переліку спеціальних технічних засобів, наприклад, таких як пристрої прослуховування, зазначено про необхідність наявності спеціального дозволу для їх використання в діяльності ОВС. Однак про засоби захисту оперативної аудіоінформації з боку правоохоронних органів у Законі не йдеться.

Авторами статті пропонується повне або часткове використання спеціального шифрувального пристрою в процесі проведення оперативно-розшукової діяльності органами внутрішніх справ.

Проаналізувавши наявні прилади та методи контролю, статистично-оперативні дані правопорушень із використанням порушниками різноманітних технічних засобів і предметів побутового використання, авторами статті запропонованою розробку та впровадження пристрою шифрування аудіоінформації в оперативно-розшуковій діяльності.

Ідею захисту інформації в контексті економічної безпеки регіону за допомогою лише технічних засобів в умовах інформаційного суспільства не можна вважати достатньо ефективною. Цей напрям можна підсилити математичними методами, що істотно при використанні криптографічних алгоритмів. Запропоновано електронно-криптографічну систему та алгоритми виконання, що використовують елементи штучного інтелекту для захисту інформації [13].

Таким чином, авторами запропоновано проект малогабаритного шифрувального пристрою, який може бути застосований у практичній діяльності оперативних підрозділів, особливо в тих випадках, коли є підозра, що в процесі проведення оперативно-розшукових заходів або операцій можуть прослуховуватись розмови оперативних працівників.

Програма для мікроконтролера AVR створюється компілятором CVAVR – CodeVisionAVR 1.25.9.

Перевірку роботи програми виконує стимулятор AVR і електроніки VMLAB [14, 5]. Використання контролера AVR не є обов'язковою умовою для реалізації СШП. Можна також використати інші типи мікроконтролерів, які за своїми параметрами відповідають вимогам до шифрувального пристрою, наприклад PIC (8-біт PIC16, PIC18, 16-біт dsPIC33/PIC24) [15] (Рис. 1).

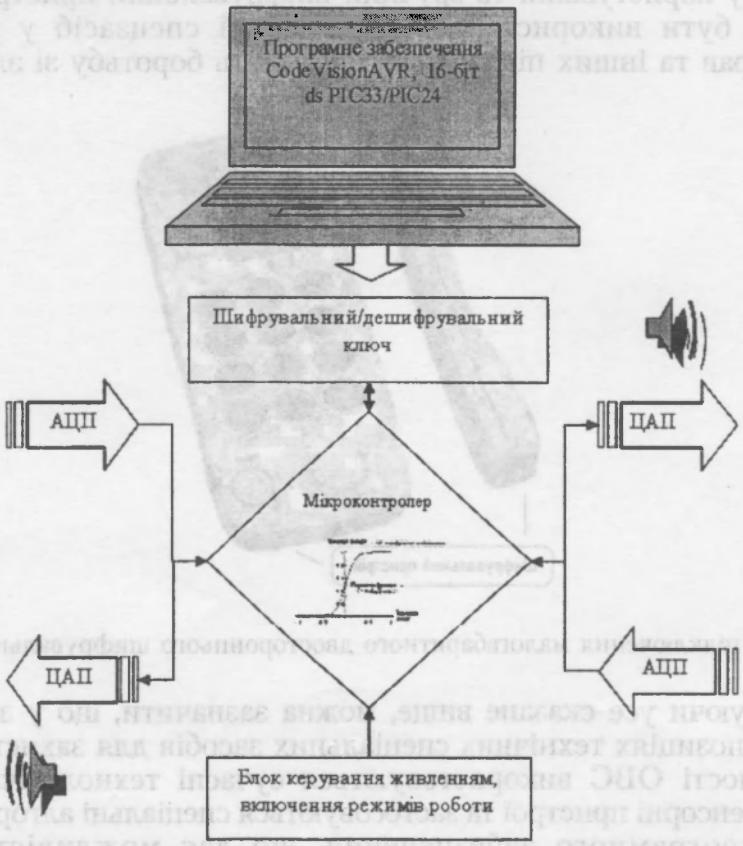

Рис. 1. Функціональна блок-схема шифрувального процесора.

Спеціальний шифрувальний пристрій має наступні переваги над наявними спеціальними засобами шифрування аудіоінформації [13]:

1) шифрувальний пристрій підключається до будь-якого телефонного апарату (мобільного або стаціонарного) в розрив між телефонною трубкою і апаратом, до мобільного телефону підключається між гарнітурою і мобільним телефоном (Рис. 2);

2) завдяки включенню шифроблоку між гарнітурою і телефоном шифрувальний пристрій дає можливість адаптувати практично всі наявні телефонні лінії зв'язку, для передачі конфіденційної інформації [18];

3) при певній модифікації, запропонований в проекті пристрій дозволяє програмним методом змінювати функцію шифрування, забезпечуючи тим самим рівень конфіденційності;

4) при використанні шифрувального пристрою під час аудіозапису, записана таким чином інформація може відтворюватись лише за наявності відповідного пристрою, а також функції зашифрованого матеріалу [19].

5) однією з важливих переваг шифрувального пристрою є те, що з пристроєм можна працювати в глобальній мережі Інтернет під час розмови по скайпу (Skype), включивши його між гарнітурою і звуковою картою персонального комп'ютера. Це можливість роботи по низькочастотному звуковому каналу комп'ютера. Таким чином, адаптується комп'ютерна мережа до передачі конфіденційних повідомлень [18].

Новітні засоби конфіденційності забезпечують використання пристрою в будь-яких умовах з умовою збереження інформації між абонентами. Крім цього, враховуючи те, що при використанні цього пристрою ні фізичні ні електричні характеристики ліній зв'язку не змінюються, певні новітні технології забезпечують гарантію закритого доступу інших технічних можливостей [20].

Простий у користуванні та зручний шифрувальний пристрій у будь-який момент може бути використаний як надійний спецзасіб у роботі органів внутрішніх справ та інших підрозділів, які ведуть боротьбу зі злочинністю.

Рис. 2. Схема підключення малогабаритного двостороннього шифрувального пристрою.

Підсумовуючи усе сказане вище, можна зазначити, що у запропонованих проектних пропозиціях технічних спеціальних засобів для захисту інформації в процесі діяльності ОВС використовуються сучасні технологічні електронно-вимірювальні сенсорні пристрої та застосовуються спеціальні алгоритми штучного інтелекту і програмного забезпечення, що дає можливість протидіяти правопорушенням на відповідному технологічному рівні.

Розроблений спеціальний шифрувальний пристрій пропонується впровадити у виробництво, як спецзасіб, та в роботу оперативних підрозділів органів внутрішніх справ.

Усі запропоновані в комплексному проекті пропозиції є авторськими розробками з науковою новизною і опубліковані лише частково.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Брюс Шнайдер.* Прикладная криптография протоколы, алгоритмы исходные тексты / Брюс Шнайдер. – М. : Триумф, 2003. – 818 с.

2. *Глибовець М.М.* Штучний інтелект / М.М. Глибовець, О.В. Олецький. – К. : Видавничий дім "КМ Академія", 2002. – 366 с.

3. *Максимов Ю.Н.* Технические методы и средства защиты информации / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров, А.В. Паршуткин, М.А. Еремеев. – Санкт-Петербург : Полигон, 2000. – 314 с.

4. Національний стандарт України, інформаційні технології, криптографічний захист. [Розроблено : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України (ДСТСЗІ СБ України), Національна академія наук України (НАН України), ЗАТ "Інститут інформаційних технологій"]. – Київ, 2006 (Проект).

5. *Смичок В.Д.* Проблеми числового диференціювання зашумлених даних аерологічних радіолокаційних вимірювань / В. Смичок, О. Бурнаєв // Вісник Львівського національного університету імені Івана Франка. Серія фізична, 2003. – Випуск 36. – Львів : Львівський національний університет імені Івана Франка. – С. 206–219.

6. *Bruce Schneier.* Kryptografia dla praktyk'ow / Bruce Schneier. – Warshawa: Wydawnictwa naukowo-technichne, 2000 – 514 p.

7. Про інформацію: Закон України від 02.10.1992 // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

8. Про державну таємницю : Закон України від 21.01.1994 [В редакції Закону від 21.09.1999 № 1079-XIV (1079-14)] // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

9. Про захист інформації в автоматизованих системах : Закон України від 05.07.1994 // Відомості Верховної Ради України, 1994. – № 31. – Ст. 286.

10. Про науково-технічну інформацію : Закон України від 25.06.1993 // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.

11. Про Службу безпеки України : Закон України від 25.03.1992 // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

12. Про міліцію : Закон України від 20 грудня 1990 // Відомості Верховної Ради України. – 1991. – № 4. – Ст. 20.

13. *Данилович В.П.* Динамічна система захисту даних на основі електронно-криптографічного протоколу шифрування / В.П. Данилович, В.Д. Смичок //Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. – Львів : ЛьвДУВС, 2010. – Вип. 1. – 391–398 с.

14. *Кауфман М.* Практическое руководство по расчетам схем в радиоэлектронике / М. Кауфман, А. Сидман. – Москва : Изд-во Энергоатомиздат., 1991. – т. 1. – 368 с.

15. *Хоровиц П.* Искуство схемотехніки / П. Хоровиц, У. Хилл. – М. : Изд-во Мир, 1998. – 703 с.

16. *Кондратьєв Я.Ю.* Науково-нрактичний коментар до Закону України "Про міліцію" / Я.Ю. Кондратьєв, І.П. Голосніченко. – К. : Українська академія внутрішніх справ, 1996. – 140 с.

17. *Шнайдер Б.* Прикладная криптографія: протоколы, алгоритмы исходные тексты / Б. Шнайдер. – М. : Триумф, 2003. – 818 с.

18. *Дмитрик Ю.І.* Використання пристрою шифрування аудіо інформації в оперативній роботі / Ю.І. Дмитрик, В.Д. Смичок // Науковий вісник Львівського державного університету внутрішніх справ. Спеціальний випуск № 1'2009. – Львів : Льв. ДУВС, 2009. – С. 78–87.

19. *Хомут О.Й.* Прилади та методи застосування штучного інтелекту / О.Й. Хомут, С.І. Федерляйн, В.Д. Смичок // Науковий вісник Львівського ДУВС. – Львів, 2007. – С. 202–211.

20. *Чигінь В.І.* Автоматична система реального часу для інформування про наявність і прогнозовану траєкторію аерологічних не пілотованих куль-зондів / В.І. Чигінь, В.П. Данилович, В.Д. Смичок, О.М. Бурнаєв // Збірник ІІІ Всеукраїнської науково-технічної конференції Академії сухопутних військ ім. П. Сагайдачного "Перспективи розвитку озброєння і військової техніки сухопутних військ", 2010. – с. 301.

Отримано 21.04.2011