

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0211U002129

Державний реєстраційний номер: 0109U008675

Особливі позначки: відкрита

Дата реєстрації: 20-01-2011

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Проведення аналізу стійкості криптосистем в залежності від типу, повноти та якості додаткової інформації

Початок етапу: 01.2010

Закінчення етапу: 12.2010

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет України "Київський політехнічний інститут", Фізико-технічний інститут

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 406-81-76

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України

Код за ЄДРПОУ: 20001993

Місцезнаходження:

Форма власності:

Сфера управління: Служба безпеки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 422-75-58

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

Напрямок фінансування: 2.1 - фундаментальні дослідження

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6521010

Фактичний обсяг фінансування (тис. грн.): 99

VII. Відомості про ДіР

Назва роботи українською:

Дослідження теоретичних основ та розробка алгоритмів впливу додаткової інформації на стійкість симетричних систем.

Назва роботи англійською:

The research of theory and development of algorithms of influence on symmetric system security additional information.

Реферат українською:

Другий етап НДР "Дослідження теоретичних основ та розробка алгоритмів впливу додаткової інформації" присвячено новітнім методам криптоаналізу з використанням додаткової інформації та побічних каналів. В результаті проведеної роботи було розглянуто та проаналізовано низку атак на симетричні та асиметричні шифри: атаки збоїв, кубічні атаки, атаки на основі гомоморфізмів, статистичні атаки на поточкові шифри, атаки компромісу тощо. Досліджено вимоги для ефективної реалізації атак на основі інформації з побічних каналів, необхідні та достатні умови стійкості криптосистем до розглянутих методів криптоаналізу, можливі способи захисту від атак з використанням додаткової інформації; розроблено декілька нових атак на сучасні шифри. Частина одержаних результатів стосується теоретичних засад криптоаналізу з використанням додаткової інформації.

Реферат англійською:

The second stage of the SRW «The research of theory and development of algorithms of influence on symmetric system security additional information» is devoted to the modern methods of cryptanalysis with the use of additional information and side channels. A number of attacks on symmetric and asymmetric ciphers were considered and analyzed: fault attacks, cube attacks, attacks on the basis of homomorphisms, statistical attacks on stream ciphers, trade-off attacks and others like that. Requirements for effective implementation of attacks on the basis of information from the side channels, necessary and sufficient conditions for the capability of cryptosystems to withstand to the considered methods of cryptanalysis, possible methods of protecting from attacks with the use of additional information; a few new attacks on modern ciphers are developed. Some of the results concern the theoretical principles of cryptanalysis with additional information.

Індекс УДК: 519.7, 681.3.06:519.248.681

Коди тематичних рубрик: 27.47

Керівники роботи

Власне Прізвище Ім'я По-батькові: Савчук Миколай Миколайович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Звіт про науково-дослідну роботу "Дослідження теоретичних основ та розробка алгоритмів впливу додаткової інформації"

Назва НТП англійською: Report of SCW "The research of tueory and development of algorithms of influence on symmetric system security additional informaiton"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 73.10.1 Дослідження і розробки в галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Досліджено системи та процеси криптографічного захисту інформації, способи створення криптоатак на системи захисту інформації. Розроблено та застосовано методи, процедури та алгоритми криптоатак на системи захисту інформації з використанням додаткової інформації. Оцінено ефективність розроблених криптографічних атак на певні типи криптосистем та способів захисту від них. Досліджено, також, методи, способи та математичні моделі криптоатак на системи захисту інформації з використанням додаткової інформації.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: -

Перспективні ринки: -

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

3 (три) статті, 8 (вісім) тезісів

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький П.О.

Завадська Л.О.

Ковальчук Л.В.

Конюшок С.

Олексійчук А.В.

Фаль О.М.

Фесенко А.В.

Шарапов В.

Яковлев С.В.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**

