Наукові результати
кафедри безпеки інформаційних технологій
за 2010-2011 н.р.

Монографії

1. Охорона державних секретів незалежної України. / **В.П.Ворожко**, Й.У.Мастяниця, Л.Є. Шиманський, О.В. Олійник — К., Інститут законодавства Верховної Ради України, 2010. — 128 с.
2. Охорона державної таємниці, як складова частина контррозвідувальної діяльності Департаменту поліції МВС Російської імперії (на прикладі українських губерній): монографія / **Б.В.Бернадський**. - К.: Наук.-вид. відділ НА СБ України, 2010. - 274 с.

Посібники з грифом МОН

1. Смірнов О.А., Віхрова Л.Г., Осадчій С.І., Мелешко Є.В., Ковтун В.Ю. Основи захисту інформації: Навчальний посібник. – Кіровоград: РВЛ КНТУ, 2011. -322 с. З грифом МОН України, Лист № 1/11-11486 від 16.12.2010 р.

Статті, опубліковані у журналах, які входять до міжнародних наукометричних баз даних (Web of Science, SCOPUS)

1. **Korchenko O.** Modern quantum technologies of information security against cyber-terrorist attacks / **O. Korchenko**, Y. Vasiliu, **S. Gnatyuk** // Aviation. Vilnius: Technika, 2010, Vol. 14, No. 2, p.58–69.

Захищені кандидатські дисертації (PhD)

1. **Гнатюк С.О.** Квантові системи захисту інформації від кібератак: дис. канд. техн. наук : 05.13.21 / **Гнатюк Сергій Олександрович**. — К., 2011. — 193 с. (захищено 10.03.2011 р.)

Міжнародні наукові конференції за кордоном на яких репрезентовано здобутки кафедри

1. III международная научно-практическая конференция "Информационные технологии в гуманитарном образовании" (РФ, Пятигорск, 2010 г.);
2. XI международная научно-практическая конференция "Информационная безопасность – 2010" (РФ, Таганрог, 2010 г.);
3. ECAC Workshop on Cyber Threats to Civil Aviation (France, Paris, 28-29 June 2011).

Навчально-методичні матеріали

1. **Корченко О.Г.**, Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів. Житомир: ЖВІ НАУ, 2010. – 280 с.

Інноваційні розробки


УКРАЇНА UKRAINE

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 43779

СИСТЕМА ПЕРЕДАЧІ КРИПТОГРАФІЧНИХ КЛЮЧІВ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.08.2009.

Голова Державного департаменту інтелектуальної власності М.В. Паладій

Патенти

1. Пат. № 43779 України, H04L 9/08. Система передачі криптографічних ключів / **Гнатюк С.О., Кінзерявий В.М., Корченко О.Г., Паціра Є.В.**; заявник та патентовласник Націон. авіаційний ун–тет. – №u200904239; заявл. 29.04.2009; опубл. 25.08.2009, Бюл. №16.

2. Пат. № 45776 України, H04L 9/06. Спосіб криптографічного перетворення інформації / **Гнатюк С.О., Кінзерявий В.М., Корченко О.Г., Паціра Є.В.**; заявник та патентовласник Націон. авіаційний ун–тет. – №u200905972; заявл. 10.06.2009; опубл. 25.11.2009, Бюл. №22.

3. Пат. № 51869 України, G09C 1/00. Спосіб формування послідовностей псевдовипадкових чисел / **Ковтун В.Ю.** Кузнецов О.О., Євсєєв С.П., Рябуха Ю.М., Щербаков О.В. – № u200913226; опубл. 10.08.2010, Бюл. № 15.

4. Пат. № 53792 України, G09C 1/00. Спосіб формування послідовностей псевдовипадкових чисел / **Ковтун В.Ю.** Кузнецов О.О., Євсєєв С.П., Рябуха Ю.М., Мінухін С.В. – № u200913201; опубл. 25.10.2010, Бюл. № 20.

5. Пат. № 45916 України, H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В.М., **Паціра Є.В.**, Миронецька І.В., Бабенко В.Г.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200907997; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. №22.

6. Пат. № 45917 України, H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В.М., **Паціра Є.В.**, Миронецька І.В., Бабенко В.Г.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. №22.

7. Пат. № 46617 України, H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В.М., **Паціра Є.В.**, Миронецька І.В., Бабенко В.Г.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. №24.

8. Пат. № 46618 України, H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В.М., **Паціра Є.В.**, Миронецька І.В., Бабенко В.Г.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. №24.

9. Пат. №55211 України, МПК H04L 9/06. Конвеєрний криптографічний обчислювач / **Корченко О.Г., Паціра Є.В.,** Панасюк А.Л., **Кінзерявий В.М., Гнатюк С.О.**; заявник та патентовласник Націон. авіаційний ун–тет. – № u20100641; Заявл. 19.05.2010; Опубл. 10.12.2010. Бюл. №23. – 8 с.

10. Пат. №55213 України, МПК H04L 9/06. Конвеєрний криптографічний обчислювач / **Корченко О.Г., Паціра Є.В.,** Панасюк А.Л., **Кінзерявий В.М., Гнатюк С.О.**; заявник та патентовласник Націон. авіаційний ун–тет. – № u20100644; Заявл. 19.05.2010; Опубл. 10.12.2010. Бюл. №23. – 8 с.

УКРАЇНА
Міністерство освіти і науки України
Державний департамент інтелектуальної власності

СВІДОЦТВО
про реєстрацію авторського права на твір
№ 36373

Комп'ютерна програма "Комп'ютерний програмний комплекс "Імітаційна модель пінг-понг протоколу в квантовому каналі з шумом"

Автори: Корченко Олександр Григорович, Василіу Євген Вікторович, Кінзерявий Василь Миколайович, Гнатюк Сергій Олександрович, Жмурко Тетяна Олександрівна

Авторські майнові права належать Одеська національна академія зв'язку ім. О.С. Попова, вул. Ковальська, 1, м. Одеса, 65029

Дата реєстрації 04.01.2011

Голова Державного департаменту інтелектуальної власності М.В.Паладій

М.П.

Авторські свідоцтва

1. Комп'ютерна програма «Модуль шифрування MCES 2010» / **Корченко О.Г., Іванченко Є.В., Гнатюк С.О., Охріменко А.О., Кінзерявий В.М., Іванченко І.С.** // Свідоцтво про реєстрацію авторського права на твір №36668 від 25.01.2011.
2. Комп'ютерний програмний комплекс «Імітаційна модель пінг-понг протоколу в квантовому каналі з шумом» / **Корченко О.Г.,** Василіу Є.В., **Кінзерявий В.М., Гнатюк С.О.,** Жмурко Т.О. // Свідоцтво про реєстрацію авторського права на твір №36373 від 04.01.2011.
3. Комп'ютерна програма «Імітаційна модель пінг-понг протоколу в квантовому каналі з шумом із застосуванням завадостійкого кодування» / **Корченко О.Г.,** Василіу Є.В., **Охріменко А.О., Гнатюк С.О., Кінзерявий В.М.** // Свідоцтво про реєстрацію авторського права на твір №37767 від 04.04.2011.
4. Комп'ютерна програма «Модуль шифрування інформації WinGost» / **Корченко О.Г.,** Лавриненко Г.С., **Кінзерявий В.М., Гнатюк С.О.** // Свідоцтво про реєстрацію авторського права на твір №36054 від 13.12.2010.
5. Комп'ютерна програма «Модуль шифрування інформації ATI_RC6» / **Корченко О.Г., Охріменко А.О., Кінзерявий В.М., Щербина В.П., Гнатюк С.О.** // Свідоцтво про реєстрацію авторського права на твір №36667 від 25.01.2011.
6. Комп'ютерна програма «AutoNotification» / Харченко В.П., **Корченко О.Г., Охріменко А.О., Гнатюк С.О., Кінзерявий В.М., Скворцов С.О.** // Свідоцтво про реєстрацію авторського права на твір №37766 від 04.04.2011.

Доповіді на міжнародних конференціях та конгресах

1. Gnatyuk S.O. Quantum computers bring new threats on confidential data / Gnatyuk S.O. // "Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК–2010)": збірка тез ІІІ Міжнародної науково-практичної конф. (24–25 травня 2010 року). – К. : НАУ, 2010. – С. 267–269.
2. Korchenko O.G. Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states / O.G. Korchenko, E.V. Vasiliu, S.V. Nikolaenko, S.O. Gnatyuk // XIII International Conference on Quantum Optics and Quantum Information (ICQOQI'2010): Book of abstracts (May 28 – June 1, 2010), P. 58–59.
3. Korchenko O. Modern directions of quantum cryptography / O. Korchenko, E. Vasiliu, S. Gnatyuk // "AVIATION IN THE XXI-st CENTURY" – "Safety in Aviation and Space Technologies": IV World Congress: Proceedings (September 21–23, 2010) – K. : NAU, 2010. – P. 17.1–17.4.
4. Ануфрієнко К. П. Огляд інтегрованих середовищ фаззінгу [Текст] / Кирило Петрович Ануфрієнко // АВІА-2011 : Матеріали X міжнародної науково-техн. конф. — К. : НАУ, 2011. — Т.1. — С. 2.14–2.17.

5. Ануфрієнко К. П. Підвищення рівня стеганографічної стійкості до суб'єктивних атак [Текст] / Павло Валентинович Сироватка, Максим Сергійович Літош, Наталія Ігорівна Довгич, Кирило Петрович Ануфрієнко // АВІА-2011 : Матеріали X міжнародної науково-техн. конф. — К. : НАУ, 2011. — Т.1. — С. 2.42–2.45.

6. Ануфрієнко К. П. Реалізація хакерських атак на веб-сайти з використанням SQL-ін'єкцій [Текст] / Кирило Петрович Ануфрієнко, Геннадій Сергійович Лавриненко // Проблеми та перспективи розвитку транспортних систем в умовах реформування залізничного транспорту: управління, економіка і технології : Матеріали V міжнародної науково-практ. конф. : Серія «Техніка, технологія». — К. : ДЕТУТ, 2011. — Т.1. — С. 222–223.

7. Ануфрієнко К. П. Характеристика програмних засобів статичного аналізу з точки зору виявлення вразливостей [Текст] / Кирило Петрович Ануфрієнко // Комп'ютерні системи та мережеві технології (CSNT-2010) : III міжнародна науково-технічна конференція : Збірник тез. — К. : Вид-во Нац. авіа. ун-ту «НАУ-друк», 2010. — С. 14.

8. Гнатюк С.О. Алгоритм побудови моделі порушника в інформаційних системах / Гнатюк С.О., Надольна М.О. // Проблеми та перспективи розвитку транспортних систем в умовах реформування залізничного транспорту: управління, економіка і технології: V міжнар. наук.-практ. конф., 24-25 березня 2011 р. : тези доп. – К. : ДЕТУТ, 2011. – С. 240-242.

9. Гнатюк С.О. Вимоги до генерації псевдовипадкових послідовностей в системах захисту інформації / Гнатюк С.О., Ясеновська В.М // Проблеми та перспективи розвитку транспортних систем в умовах реформування залізничного транспорту: управління, економіка і технології: V міжнар. наук.-практ. конф., 24-25 березня 2011 р. : тези доп. – К. : ДЕТУТ, 2011. – С. 240-242.

10. Гнатюк С.О. Загальні принципи побудови абстрактної моделі порушника інформаційної безпеки / С.О. Гнатюк, М.О. Надольна // ПОЛІТ–2011. Сучасні проблеми науки : IX міжнар. наук.-практ. конф. молодих учених і студентів, 6-7 квітня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С. 153–154.

11. Гнатюк С.О. Стеганографічні методи захисту інформаційних технологій / Гнатюк С.О., Довгич Н.І., Літош М.С. // Проблеми та перспективи розвитку транспортних систем в умовах реформування залізничного транспорту: управління, економіка і технології: V міжнар. наук.-практ. конф., 24-25 березня 2011 р. : тези доп. – К. : ДЕТУТ, 2011. – С. 239-240.

12. Гнатюк С.О. Абстрактна модель порушника у квантових системах захисту інформації / С.О. Гнатюк // Захист інформації з обмеженим доступом та автоматизація її обробки: III наук.-техн. конф., 8-9 лютого 2011 р. : тези доп. – К. : НАУ, 2011. – С. 4–5.

13. Гнатюк С.О. Базові аспекти забезпечення безумовної стійкості квантово-криптографічних систем / С.О. Гнатюк // "Комп'ютерні системи та мережні технології" (CSNT 2010) : III Міжнародна науково-технічна конференція : тези доповідей (15–17 червня 2010 року) – К. : НАУ, 2010. – С. 29.

14. Гнатюк С.О. Базові ознаки класифікації кібератак на квантові системи захисту інформації / С.О. Гнатюк, С.О. Демченко, В.М. Кінзерявий // АВІА-2011 : X міжнар. наук.-техн. конф., 19-21 квітня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту "НАУ-друк", 2011. – С. 2.26–2.30.

15. Гнатюк С.О. Використання технологій паралельної обробки даних в криптографічних перетвореннях / С.О. Гнатюк, А.О. Охріменко // Захист інформації з обмеженим доступом та автоматизація її обробки: III наук.-техн. конф., 8-9 лютого 2011 р. : тези доп. – К. : НАУ, 2011. – С. 11–12.

16. Гнатюк С.О. Використання тритових псевдовипадкових послідовностей в криптографії / С.О. Гнатюк, Т.О. Жмурко // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК–2011) : IV Міжнар. наук.-практ. конф., 23-25 травня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С. 414–416.

17. Гнатюк С.О. Впровадження режиму шифрування CTR у мережевий протокол аутентифікації CERBEROS / С.О. Гнатюк, Довгич Н.І., Літош М.С. // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК–2011) : IV Міжнар. наук.-практ. конф., 23-25 травня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С. 405–408.

18. Гнатюк С.О. Критерії оцінки стійкості криптографічних систем захисту інформації / С.О. Гнатюк, Ю.Є. Хохлачова // АВІА-2011 : X міжнар. наук.-техн. конф., 19-21 квітня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту "НАУ-друк", 2011. – С. 2.22–2.26.
19. Гнатюк С.О. Підвищення рівня стеганографічної стійкості за рахунок використання методу синонімічних замін / С.О. Гнатюк, П.В. Сироватка // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК–2011) : IV Міжнар. наук.-практ. конф., 23-25 травня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С. 430–432.
20. Гнатюк С.О. Сучасні підходи до вирішення проблеми розподілу ключів шифрування / С.О. Гнатюк // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК–2011) : IV Міжнар. наук.-практ. конф., 23-25 травня 2011 р. : тези доп. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С. 400–402.
21. Корченко О.Г. Систолический криптопроцессор / Корченко О.Г., Гнатюк С.О., Кінзерявий В.М., Панасюк А.Л. // «Інформаційні технології та комп'ютерна інженерія»: тези доповідей Міжнародної науково–практ. конф. (19–21 травня 2010 року). – Вінниця : ВНТУ, 2010. – С. 187–189.

Статті у виданнях ВАК України та СНД

1. Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika, 2010, Vol. 14, No. 2, p.58–69.
2. Korchenko O.G., Vasiliu E.V., Gnatyuk S.O. Modern quantum technologies of information security, Cornel University Library, arXiv: 1005.5553v2 [cs.CR].
3. Kovtun V. Software Implementation of Genus-2 Hyperelliptic Curve Cryptosystems Over Prime Fields/ Kovtun V., Kuznetsov A., Evseev S. // Сучасний захист інформації. Науково-технічний журнал. –Київ: ДУІКТ, 2010.-Вип. 3. –с. 39-51.
4. Kovtun V. Use of Complex Discrete Signals for Steganograpic Information Security / Kuznetsov A., Srhiienko R., Kovtun V., Botnov A. // Statistics Methods of Signal and Data Processing (SMSDP-2010): Proceedings. Kiev, Ukraine, October 13-14, 2010 / General Chairman I. Prokopenko. –Kiev: National Aviation University "NAU-Druk" Publishing House, 2010. –p. 143-147.
5. Ануфрієнко К. П. Категоризація методик фаззінгу [Текст] / К. П. Ануфрієнко, В. В. Бобровський, Д. В. Луценко, О. В. Григоренко // Захист інформації. — 2010. — № 4. — С. 17–23.
6. Ануфрієнко К. П. Порівняльний аналіз фаззінгових фреймворків [Текст] / М. Г. Луцький, М. М. Чепілко, К. П. Ануфрієнко // Захист інформації. — 2011. — № 1. — С. 101–105.
7. Бернадський Б.В. Ставлення органів державної безпеки Російської імперії до Римо-католицької Церкви у Правобережній Україні (1905 - 1914 рр.) // Записки Українського католицького університету. Серія: Історія. Число 1.-Львів,2010.-С.133-147.
8. Бернадський Б.В. Український рух очима політичної поліції // Педагогічний орієнтир. - 2011.- №1 (15).- с.10-14; №2 (16).- с.22-28.
9. Ворожко В.П. Щодо розсекречування архівних документів у сучасній Україні / В.П.Ворожко, О.Б.Пащенко // К., Студії з архівної справи та документознавства, №18, 2010 — С.32-36
10. Дрейс Ю.О., Вишневська Н.С., Хохлачова Ю.Є. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю. Захист інформації: науково-технічний журнал. Вип.3/ Інститут інформаційно-діагностичних систем Національного авіаційного університету. – К.: ДУІКТ, 2010р. – С. 10 –14.
11. Ковтун В.Ю. Формула сложения дивизоров с идентичными Z-координатами в якобиане гиперэллиптической кривой второго рода над простыми полями // Захист інформації. Науково-технічний журнал. –Київ: НАУ, 2010. –Вип. 3(48). –с. 81-87.
12. Корченко О.Г. Квантово-криптографічна система з безумовною стійкістю / О.Г. Корченко, С.О. Гнатюк, О.В. Васько, С.П. Козирев // Захист інформації. – №2, 2010. – С. 43–49.
13. Корченко О.Г. Швидкодіючий конвеєрний криптографічний обчислювач / Корченко О.Г., Панасюк А.Л., Гнатюк С.О., Кінзерявий В.М. // Вісник Східноукраїнського національного університету імені Володимира Даля – №5 (159), 2011. – С. 317–320.

14. Корченко О.Г., Дрейс Ю.О. Визначення рівня компетентності експертів експертної комісії з питань державної таємниці. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. – Житомир: ЖВІ НАУ, 2011. – Вип. 4. – С.190-196.
15. Корченко О.Г., Дрейс Ю.О., Ходаківський В.М. Спецтема. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. – Житомир: ЖВІ НАУ, 2010. – Спецвипуск 1. – С.69-77.
16. Корченко О.Г. Атаки в квантових системах захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. – №2, 2010. – С. 109–115.
17. Корченко О.Г. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. – №3, 2010. – С. 46–56.
18. Корченко О.Г. Оцінка корегувальної здатності завадостійких трійкових РС-кодів при передачі інформації повністю переплутаними станами кутритів квантовим каналом із шумом / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий, Горчинська А.М. // Захист інформації. – №4, 2010. – С. 44–53.
19. Рындюк В.А. Альтернативные средства конфиденциальной связи /В.А. Рындюк, А.Г. Корченко, С.А. Гнатюк, В.Н. Кинзерявый // "Информационные технологии в гуманитарном образовании" им. Т.П. Сарана: III Международная научно-практическая конференция: сборник статей по материалам докладов конференции – Пятигорск: ПГЛУ, 2010. – С. 357–363.
20. Стасюк О.І. Сучасні стеганографічні методи захисту інформації / Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. // Захист інформації. – 2011. – №1 (50). – С. 56–63.
21. Ткаченко В.В. «Дорожная карта» специалиста по информационной безопасности Оцінка корегувальної здатності завадостійких трійкових РС-кодів при передачі інформації повністю переплутаними станами кутритів квантовим каналом із шумом / В.В. Ткаченко, С.В. Карпенко, С.О. Гнатюк, Т.М. Артеменко // Захист інформації. – №4, 2010. – С. 35–44.