Облікова картка НДДКР

Державний обліковий номер: 0216U002637

Державний реєстраційний номер: 0114U004275

Відкрита

Дата реєстрації: 05-05-2016

1. Етапи виконання

Номер етапу: 1

Назва етапу: Вибір напряму дослідження. Теоретичні та експериментальні дослідження. Оцінювання результатів досліджень. Підготовка звіту за темою.

Початок етапу: 01-2014

Закінчення етапу: 12-2015

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Львівський державний університет безпеки життєдіяльності

Код ЄДРПОУ/ІПН: 08571340

Підпорядкованість: Державна служба України з надзвичайних ситуацій

Адреса: м. Львів, вул. Клепарівська, 35

Телефон: 233-00-88

E-mail: ndr@ubgd.lviv.ua; yaroslav_kyryliv@ukr.net

3. Власник результатів НДДКР (продукції)

Назва організації: Львівський державний університет безпеки життєдіяльності

Код ЄДРПОУ/ІПН: 08571340

Адреса: вул. Клепарівська, 35, м. Львів, Львівська обл., 79007, Україна

Підпорядкованість: Державна служба України з надзвичайниїх ситуацій

Телефон: 380671778187

Телефон: 0322330088

E-mail: ldubzh.lviv@mns.gov.ua

4. Джерела та напрями фінансування

Підстава для проведення робіт: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

КПКВК:

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

Джерело фінансування: 7704 - власні кошти, кошти підприємств, установ, організацій, фізичної особи на виконання ініціативних робіт

Фактичний обсяг фінансування за звітний етап: 35 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України

Назва роботи (англ)

Development of methods and models for information and communication systems and networks in subdivisions DSNS Ukraine

Реферат (укр)

Звіт про науково-дослідну роботу: 57 стор., 10 рис., 10 табл., 3 розділи. Сучасні темпи розвитку інформаційних технологій вимагають від працівників структурних підрозділів ДСНС України високого рівня захисту конфіденційної інформації. Колективне використання інформаційних ресурсів потребує відповідного захисту дисків і каталогів, окремих папок і файлів, а також усіх локальних і глобальних мереж від несанкціонованого втручання інформаційних зловмисників, вірусів і небезпечних програм. Найважливішим завданням на цьому рівні є фізичний захист самого інформаційного ресурсу. Якщо ж на такому ресурсі зберігаються конфіденційні дані, то він має бути надійно захищеним за допомогою вбудованих засобів операційних систем, апаратного та програмного забезпечення. При цьому важливим є забезпечення належного функціонування системи захисту інформації шляхом регулярного аналізу приміщень структурних підрозділів ДСНС України, у яких розташовуються інформаційні ресурси колективного користування. Метою цієї роботи є з'ясування теоретичних особливостей та розроблення сучасних ефективних методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України. Об'єктом дослідження є конфіденційність інформації та захищеність інформаційно-комунікаційні системи і мереж, наявних у структурних підрозділах ДСНС України. Предметом дослідження є методи і моделі захисту інформаційно-комунікаційних систем і мереж. Методи дослідження. В роботі використано методику визначення джерел загроз безпеці інформаційно-комунікаційних систем, методику формування моделі загроз та порушника і методику реалізації політики безпеки підприємства. Ключові слова: інформаційно-комунікаційні системи і мережі, методи захисту, комплексна система захисту інформації.

Реферат (англ)

The report on the research work: 57 p., 10 fig., 10 tab., 3 sections. Modern pace of development of information technologies require the employees of structural units DSNS Ukraine high level of protection of confidential information. Collective use of information resources requires appropriate protection drives and directories, folders and files, as well as all local and global networks from unauthorized interference Information intruders, viruses and dangerous programs. The most important task at this level is the physical protection of the information resource. If on this website are stored sensitive data, it should be protected by using built-in operating systems, hardware and software. It is important to ensure proper functioning of the information security space through regular analysis of structural units DSNS Ukraine, in which information resources are shared use. The aim is to clarify the theoretical characteristics and the development of modern efficient methods and models for the protection of information and communication systems and networks in the structural units DSNS Ukraine. Object is a privacy and security of information and communication systems and networks, existing structural units DSNS Ukraine. The subject of research is the methods and models of protection of information and communication systems and networks. Research methods. The paper used method for determining the sources of threats to the security of information and communication systems, methods of forming patterns of threats and the offender and method of implementing the security policy of the company. Key words: information and communication systems and networks, methods of protection, a comprehensive system of data protection.

Індекс УДК: 004.7, 004.56.5 (043.2)

Коди тематичних рубрик НТІ: 50.09.53

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України

Назва продукції (англ): Development of methods and models for information and communication systems and networks in subdivisions DSNS Ukraine

Очікувані результати: Нормативно-технічна документація

Галузь застосування: КВЕД К 74.60.0

Опис продукції (укр): Забезпечити безперебійну роботу структурних підрозділів ДСНС України, тобто звести до мінімуму нанесені збитки від потенційних джерел загроз як конфіденційній інформації, так і іншим інформаційним ресурсам шляхом їхнього передбачення, випередження чи запобігання. Управління інформаційною безпекою дає змогу колективно використовувати будь-яку конфіденційну інформацію та відповідні інформаційні ресурси, забезпечуючи при цьому їх ефективний захист від несанкціонованого доступу зловмисників.

Соціально-економічна спрямованість НТП:

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження: 06.15 по 04.16

Виробник продукції: ЛДУБЖД

Споживачі продукції: ДСНС України, наукові установи та вищі навчальні заклади

Перспективні ринки: Україна та інші країни світу

Права інтелектуальної власності: «Ноу-хау»

Форми та умови передачі продукції: Продаж «Ноу-хау»

7. Бібліографічний опис

1. Грицюк Ю.І. Комплексне оцінювання проектів впровадження системи захисту інформації / Ю. І. Грицюк, І. С. Кузьменко // Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування . - 2013. - № 774. - С. 39-50. - Режим доступу: http://nbuv.gov.ua/j-pdf/VNULP_2013_774_9.pdf. 2. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року N 851-IV // Із змінами і доповненнями, внесеними Законом України від 31 травня 2005 року N 2599-IV. 3. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23 лютого 2006 року N 3475-IV // Із змінами і доповненнями, внесеними Законами України станом від 15 січня 2009 року N 879-VI.

8. Звітна документація

Кількість сторінок в звіті: 57

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Берегулько Наталія Олександрівна

Кузьменко Ірина Сергіївна

Лагун Андрій Едуардович

Полотай Орест Іванович

Самотий Володимир Васильович

Керівник організації:

Козяр Михайло Миколайович

Керівники роботи:

Грицюк Юрій Іванович

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.