# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0517U000802

**Особливі позначки:** відкрита

**Дата реєстрації:** 05-12-2017

**Статус:** Захищена

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Гнатюк Сергій Олександрович
2. Gnatyuk Sergiy

**Кваліфікація:**

**Ідентифікатор ORCID ID:** Не застосовується

**Вид дисертації:** доктор наук

**Аспірантура/Докторантура:** ні

**Шифр наукової спеціальності:** 05.13.21

**Назва наукової спеціальності:** Системи захисту інформації

**Галузь / галузі знань:** Не застосовується

**Освітньо-наукова програма зі спеціальності:** Не застосовується

**Дата захисту:** 30-11-2017

**Спеціальність за освітою:** 8.160102

**Місце роботи здобувача:** Національний авіаційний університет

**Код за ЄДРПОУ:** 01132330

**Місцезнаходження:** 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

## III. Відомості про організацію, де відбувся захист

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** Д 26.062.17

**Повне найменування юридичної особи:** Національний авіаційний університет

**Код за ЄДРПОУ:** 01132330

**Місцезнаходження:** пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

## IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

**Повне найменування юридичної особи:** Національний авіаційний університет

**Код за ЄДРПОУ:** 01132330

**Місцезнаходження:** 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

## V. Відомості про дисертацію

**Мова дисертації:**

**Коди тематичних рубрик:** 73.37.17

### Тема дисертації:

1. Методологія підтримки процесів формування та забезпечення державної системи кібербезпеки в галузі цивільної авіації

2. Methodology for support the state cybersecurity system forming and providing in civil aviation

### Реферат:

1. Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми створення методології підтримки процесів формування та забезпечення державної системи КБ в галузі ЦА на основі розроблених теоретичних основ, методів, моделей та засобів забезпечення захисту КАІС. У роботі запропоновано базову модель формування вимог до забезпечення КБ ЦА, що дала можливість формалізувати процес створення повної множини вимог, які необхідно виконати для захисту ЦА від КБЗ. Розроблено мультирівневу модель даних, яка дозволяє формалізувати процес ідентифікації виконання вимог та визначення режимів безпеки КАІС. Також розроблено метод визначення рівня критичності систем, який дозволяє оцінювати рівень важливості і ранжувати КАІС за кількісними параметрами. Розроблено метод управління інцидентами КБ, який дозволяє прогнозувати категорії інцидентів КБ, що виникнуть внаслідок реалізації певної КБА, та їх рівень небезпеки для КАІС. Створено метод симетричного криптографічного захисту інформації та новий БШ найого основі, що дозволило забезпечити захищеність КАІС від КБА ЛДК,

отримати аналітичні верхні оцінки параметрів, які характеризують його практичну стійкість. Крім того, удосконалено квантово-криптографічні методи підтримки процесів розподілу ключів та КПБЗ, які дали можливість забезпечити конфіденційність процесу розподілу ключів шифрування між легітимними користувачами та збільшити швидкість передавання даних при збереженні стійкості до некогерентних КБА. Розроблено метод оцінювання, який дає можливість визначати кількісні параметри, що характеризують повноту виконання множини вимог щодо КБ ЦА. Розроблено методологію підтримки процесів формування та забезпечення державної системи КБ в галузі ЦА, яка дозволяє забезпечити підтримку процесів формування державної системи КБ ЦА з урахуванням вимог керівних органів, визначити повноту виконання таких вимог, а також на системному рівні забезпечити процес захисту ЦА від КБЗ.

2. Thesis is devoted to solving actual scientific and practical problem of development the methodology for support the state cybersecurity (CS) system forming and providing in civil aviation (CA). This methodology is grounded on developed theoretical bases, methods and specialized tools for CS of critical aviation information systems (CAIS). Basic model for CS requirements forming was proposed and allowed to formalize CS requirements complete set forming process in CA. On the base of this model the techniques for creation domestic CS requirements complete set was developed to form Ukrainian state CS system in CA. Also the multilevel data model for CS requirements providing identification was developed. It can be used to define security modes of CAIS in accordance to selected CS model or in multilevel mode. Theory of CS in CA was developed and generalized terms of key concept in this field were defined, practical recommendations for state CS strategy from viewpoint of CIIP were formulated, conceptual ontology and classifications were also fulfilled. Method and software tool for CAIS criticality evaluation were proposed and these allow to calculate quantitative parameters of criticality and rank different CAIS. CS incident management method was proposed and realized using NSL-KDD base to forecast CS incidents categories (in accordance with practical guidelines, standard, company or state recommendations) and resulted threats for CAIS. It should be useful for CERT / CSIRT centers' activity in a part of CS incidents prioritization and adequate respond. Symmetric encryption method for CAIS security against linear and differential cryptoanalisys was developed. Also block cipher Luna-2k17 was proposed and realized in form of console software and it provides high cryptographic transformation rate; cipher was successfully checked by NIST STS and Diehard tests. Quantum cryptography methods were improved to support key distribution and secure direct communication processes. Experimental study of these methods confirms growing data transmission rate by high capacity deterministic protocols. Also assessment method for quantitative parameters defining was developed for completeness evaluation in process of CS requirements providing in CA. On the base of this method software application was designed and the completeness of Ukrainian CA was evaluated. Finally the methodology for support the state CS system forming and providing in CA was developed and allowed to provide state CS system forming in CA, define completeness of requirements providing and also provide CS of CA on system level.

**Державний реєстраційний номер ДіР:**

**Пріоритетний напрям розвитку науки і техніки:**

**Стратегічний пріоритетний напрям інноваційної діяльності:**

**Підсумки дослідження:**

**Публікації:**

**Наукова (науково-технічна) продукція:**

**Соціально-економічна спрямованість:**

**Охоронні документи на ОПІВ:**

**Впровадження результатів дисертації:**

**Зв'язок з науковими темами:**

## VI. Відомості про наукового керівника/керівників (консультанта)

**Власне Прізвище Ім'я По-батькові:**

1. Корченко Олександр Григорович
2. Korchenko Oleksandr

**Кваліфікація:** д.т.н., 05.13.21

**Ідентифікатор ORCID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

## VII. Відомості про офіційних опонентів та рецензентів

**Офіційні опоненти**

**Власне Прізвище Ім'я По-батькові:**

1. Лахно Валерій Анатолійович
2. Лахно Валерій Анатолійович

**Кваліфікація:** д.т.н., 05.13.21

**Ідентифікатор ORCID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Власне Прізвище Ім'я По-батькові:**

1. Міщенко Андрій Віталійович
2. Міщенко Андрій Віталійович

**Кваліфікація:** д.т.н., 21.05.01

**Ідентифікатор ORCID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Власне Прізвище Ім'я По-батькові:**

1. Александер Марек Богуслав
2. Александер Марек Богуслав

**Кваліфікація:** д.т.н., 05.13.21

**Ідентифікатор ORCID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Рецензенти**

## VIII. Заключні відомості

| | |
|---|---|
| **Власне Прізвище Ім'я По-батькові голови ради** | Корченко Олександр Григорович |
| **Власне Прізвище Ім'я По-батькові головуючого на засіданні** | Корченко Олександр Григорович |
| **Відповідальний за підготовку облікових документів** | |
| **Реєстратор** | |

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

Юрченко Т.А.