Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0414U001821

Особливі позначки: відкрита

Дата реєстрації: 08-05-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Олешко Інна Вікторівна
2. Oleshko Inna Viktorivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

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: 08-04-2014

Спеціальність за освітою: 8.160101

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

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): К 64.052.05

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Моделі та методи оцінки захищеності механізмів багатофакторної автентифікації від несанкціонованого доступу

2. Models and methods for assessing security of multi-factor authentication mechanisms from unauthorized access

Реферат:

1. Мета дисертаційного дослідження - розробка математичних моделей та методів оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації та порівняльний аналіз механізмів багатофакторної автентифікації, що дозволяє мінімізувати ймовірності НСД щодо інформації та ресурсів. Запропоновано математичні моделі оцінки захищеності від НСД інформації та ресурсів з використанням механізмів багатофакторної автентифікації, які базуються на обчисленні ймовірностей НСД та безвідмовної роботи механізмів, що дозволяє оцінити ймовірності НСД у схемах багатофакторної автентифікації. Запропоновано методи оцінки захищеності від НСД з використанням механізмів багатофакторної автентифікації, які базуються на визначенні повного переліку атак відносно аналізованого фактора, їх класифікації, аналізу критеріїв та показників, які дозволяють їх порівняти та вибору таких атак, які можуть бути реалізовані та забезпечували б досягнення максимальних значень складностей

криптоаналізу, що дозволяє оцінити ймовірності НСД як під час використання кожного фактора окремо, так і в схемах багатофакторної автентифікації взагалі. Запропоновано ентропійну модель райдужної оболонки ока, яка базується на визначенні кількості інформації, яка міститься в райдужній оболонці, що дозволяє обчислити кількість біометричної інформації райдужки та порівнювати не тільки біометричні ознаки між собою, але і з ПІН-кодом, паролем та іншими методами автентифікації в ході використання їх ентропійних оцінок. Удосконалено метод автентифікації, який описано в стандарті ДСТУ ISO/IEC 9798-5, що відрізняється від існуючого тим, що замість перетворень у мультиплікативній групі поля використовуються перетворення у групі точок еліптичної кривої, що дозволяє досягти експоненціального рівня складності здійснення атаки "повне розкриття", а також зменшити довжини ключа при збереженні показника безпечного часу.

2. The dissertation is devoted to development of mathematical models and methods for assessing information and resources security from unauthorized access using multi-factor authentication (MFA) mechanisms and comparative analysis of MFA mechanisms to minimize the probability of unauthorized access to information and resources. This paper describes mathematical models for assessing information and resources security from unauthorized access using MFA mechanisms based on the calculation of unauthorized access probabilities and uptime probabilities to estimate unauthorized access probabilities for multi-factor authentication schemes. Also it describes methods for assessing security from unauthorized access using MFA mechanisms based on attacks complete list determining against this factor, attacks classification, analysis of criteria and indicators compare and choose from such attacks, which can be implemented and would ensure the achievement of the maximum complexity values of cryptanalysis. These methods allow to estimate unauthorized access probabilities as using each factor separately and in a MFA schemes in general. Here we propose the iris entropy model based on the quantity of information contained in the iris, which allows to calculate the amount of iris biometric information and compare not only the biometric features among themselves but also with the PIN, password and other authentication means by using their entropy estimates. Also we improve ISO/IEC 9798-5 authentication method by changing transformations in the multiplicative group to the group of points of an elliptic curve to achive the exponential complexity for the "full disclosure" attack, as well as reduce key length while preserving the safety time.

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. Горбенко Іван Дмитрович

2. Gorbenko Ivan Dmytrovych

Кваліфікація: д.т.н., 20.01.09

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. Харченко В'ячеслав Сергійович
2. Харченко В'ячеслав Сергійович

Кваліфікація: д.т.н., 20.02.14

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. Проскуровський Роман Васильович
2. Проскуровський Роман Васильович

Кваліфікація: к.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 Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.