

УКРАЇНА



ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ
№ 143963

СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ
ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОДОВЖЕНИХ КОДІВ З
НАНЕСЕННЯМ ЗБИТКУ

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

Зареєстровано в Державному реєстрі патентів України на корисні моделі **25.08.2020**.

Заступник Міністра розвитку економіки, торгівлі та сільського господарства України

Д.О. Романович



(21) Номер заявки: **u 2020 00756**
(22) Дата подання заявки: **07.02.2020**
(24) Дата, з якої є чинними права на корисну модель: **25.08.2020**
(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **25.08.2020, Бюл. № 16**

(72) Винахідники:
Євсєєв Сергій Петрович, UA,
Циганенко Олексій Сергійович, UA,
Король Ольга Григорівна, UA,
Корольов Роман Володимирович, UA,
Гаврілова Алла Андріївна, UA,
Шматко Олександр Віталійович, UA,
Хвостенко Владислав Сергійович, UA,
Ткачов Андрій Михайлович, UA,
Погасій Сергій Сергійович, UA,
Меленті Євген Олександрович, UA

(73) Власники:
Євсєєв Сергій Петрович,
вул. Героїв Праці, б. 21а, кв. 26, м. Харків, 61144, UA,
Циганенко Олексій Сергійович,
вул. Котляревського 7, смт Нова Водолага, Харківська обл., 63202, UA,
Король Ольга Григорівна,
вул. Героїв Праці, б. 21а, кв. 26, м. Харків, 61144, UA,
Корольов Роман Володимирович,
просп. Науки, 22А, кім. 449, м. Харків, 61072, UA,
Гаврілова Алла Андріївна,
вул. Спартака, б. 16, кв. 33, м. Харків, 61001, UA,
Шматко Олександр Віталійович,
вул. Дружби Народів, 267, кв. 181, м. Харків, 61183, UA,
Хвостенко Владислав Сергійович,
пр. Людвіга Свободи, 42, кв. 7, м. Харків, 61204, UA,
Ткачов Андрій Михайлович,
пр. Московський, 210/4, кв. 1, м. Харків, 61082, UA,
Погасій Сергій Сергійович,
вул. Світланівська, 14, м.

(11) **143963**

Харків, 61157, UA,
Меленті Євген
Олександрович,
пр. Московський, 264, кв. 198,
м. Харків, 61082, UA

(54) Назва корисної моделі:

**СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ
ПОДОВЖЕНИХ КОДІВ З НАНЕСЕННЯМ ЗБИТКУ**

(57) Формула корисної моделі:

Спосіб криптографічного перетворення інформації з використанням подовжених кодів з нанесенням збитку, який полягає в тому, що інформаційні дані перетворюють у кодове слово, яке маскується під випадкову послідовність (криптограму) за допомогою пристроїв кодування замаскованого лінійного блокового (n, k, d) еліптичного коду над $GF(q)$, який **відрізняється** тим, що в канал зв'язку надходить кодове слово, скорочене за рахунок видалення визначених символів за допомогою вектора ініціалізації IV_2 , до якого додаються символи відкритого тексту, які визначаються вектором ініціалізації IV_3 , наноситься збиток універсальним механізмом збитку та використовується додатковий вектор ініціалізації IV_1 для фіксації множини відкритих текстів, непридатних для використання.

(11) **143963**

Державне підприємство
«Український інститут інтелектуальної власності»
(Укрпатент)

Цей паперовий документ ідентичний за документарною інформацією та реквізитами електронному документу з електронним підписом уповноваженої особи Міністерства розвитку економіки, торгівлі та сільського господарства України.

Паперовий документ містить 3 арк., які пронумеровані та прошиті металевими люверсами.

Для доступу до електронного примірника цього документа з ідентифікатором 2712210820 необхідно:

1. Перейти за посиланням <https://sis.ukrpatent.org>.
2. Обрати пункт меню Сервіси – Отримати оригінал документу.
3. Вказати ідентифікатор електронного примірника цього документа та натиснути «Завантажити».

Уповноважена особа Укрпатенту

25.08.2020



І.Є. Матусевич