УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

03056, м. Київ, пр-т Перемоги, 37; тел. (+38 044) 204-82-82 тел./факс (+38 044) 204-97-88
http://www.kpi.ua e-mail: mail@kpi.ua ЄДРПОУ 02070921

_____ № _____
на № _____ від _____

Комітет з державних премій України
в галузі науки і техніки

ДОВІДКА

про творчий внесок кандидата технічних наук, доцента кафедри фізико-технічних засобів захисту інформації Фізико-технічного інституту **Прогонова Дмитра Олександровича** в роботі «**Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі**» для участі в конкурсі на здобуття Премії президента України для молодих вчених

Прогонов Дмитро Олександрович зарекомендував себе як перспективний молодий науковець, що займається розробкою методів стегоаналізу мультимедійних даних, зокрема цифрових зображень. На момент виконання роботи (2012-2017 рр.) Прогонов Д.О. навчався у магістратурі (2012-2013 рр.) і аспірантурі (денна форма навчання, 2013-2016 рр.), працював на кафедрі фізико-технічних засобів захисту інформації (з 2017 р.) Фізико-технічного інституту НТУУ «КПІ ім. Ігоря Сікорського». У фокусі його наукової уваги перебувають питання пов'язані з забезпеченням надійного виявлення прихованих повідомлень (стеганограм), а також відновлення процесу вбудовування стегоданих за наявності обмежених або відсутності апріорних даних щодо використаного стеганографічного алгоритму.

Автором проведено низку фундаментальних досліджень в галузі стегоаналізу цифрових зображень, які стосуються визначення меж практичного застосування відомих методів статистичного та універсального стегоаналізу. Для підвищення імовірності виявлення стеганограм у найбільш складних випадках пасивного стегоаналізу, Прогоновим Д.О. вперше запропоновано використовувати багаторівневу модель зображення-контейнеру, що відрізняється врахуванням не тільки власних шумів зображення, а й контурів та об'єктів на зображення. Автором вдосконалено потужні методи структурного аналізу зображень, зокрема варіограмий, флуктуаційний та мультифрактальний аналіз, для виявлення слабких спотворень окремих компонентів зображення-контейнеру, обумовлених приховуванням повідомлень.

Прогоновим Д.О. розроблено методику проведення стегоаналізу цифрових зображень, що заснована на інтегральному застосуванні запропонованої багаторівневої моделі та вдосконалених методів структурного аналізу, та створено комплекс прикладних програм для підтримки її реалізації. Вагомою перевагою запропонованої методи у порівнянні з існуючими аналогами є визначення особливостей використаного стеганографічного алгоритму, зокрема кількості та типу перетворень зображення-контейнеру та стегоданих, та реконструкція процесу формування стеганограм. Це дозволяє обирати ефективні методи деструкції прихованих повідомлень при забезпеченні мінімальних візуальних спотворень стеганограм.

Одержані результати у наукових працях Прогонова Д.О. дозволяють принципово підвищити рівень захищеності інформаційно-комунікаційних систем державних організацій і приватних підприємств, та є підґрунтям для подальшого розроблення складових елементів системи національної безпеки України у частині виявлення і протидії використання кібернетичної зброї.

Результати роботи впроваджено у практичну діяльність в Особливому конструкторському бюро «Шторм» НТУУ «КПІ ім. Ігоря Сікорського», в навчальний процес кафедри фізико-технічних засобів захисту інформації Фізико-технічного інституту НТУУ «КПІ ім. Ігоря Сікорського», що підтверджується відповідними довідками та актами. Одержані наукові та практичні результати були використані при виконанні держбюджетних НДР, в яких автор був виконавцем: «Дослідження та застосування методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних. НДР «Кета» (держ. реєстр. № 0114U004643); «Комплекс синергетичної фізіотерапії з регулюванням параметрів за даними діагностики та моніторингу функціонального стану людини» (держ. реєстр. № 0114U00557).

Результати досліджень за темою роботи викладено у 56 наукових працях, з них: 6 статей у фахових наукових виданнях України з технічних наук, із них 6 – в співавторстві; 3 статті у зарубіжних наукових виданнях з технічних наук, із них 1 – у співавторстві; 47 тез доповідей міжнародних та всеукраїнських наукових конференцій. Частка, виконана особисто претендентом у роботі, яка подається на здобуття премії Президента України для молодих вчених, складає 33,3%. Враховуючи необхідність неухильного дотримання норм наукової етики, автор не використовує ідеї та напрацювання, які належать співавторам.

У виданнях, внесених до наукометричних баз DOAJ, DOI, Google Scholar, Index Copernicus, ROAD та інших, розміщено 9 публікацій. Загальна кількість посилань на публікації автора складає 26 (згідно з базою даних Google Scholar), h-індекс рівний 3.

Роботу «Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі » не було удостоєно державних нагород раніше.

Проректор з наукової роботи **М.Ю. Ільченко**

УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
03056, м. Київ, пр-т Перемоги, 37; тел. (+38 044) 204-82-82 тел./факс (+38 044) 204-97-88
http://www.kpi.ua e-mail: mail@kpi.ua ЄДРПОУ 02070921

_____ № _____
на № _____ від _____

Комітет з державних премій України
в галузі науки і техніки

ДОВІДКА

про творчий внесок кандидата технічних наук, доцента кафедри математичних методів захисту інформації Фізико-технічного інституту **Яковлєва Сергія Володимировича** в роботі «**Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі**» для участі в конкурсі на здобуття Премії президента України для молодих вчених

Яковлєв Сергій Володимирович зарекомендував себе як перспективний молодий науковець, що займається методами криптографічного аналізу симетричних шифрів та геш-функцій та доведення стійкості до криптографічних атак. На момент виконання роботи (2012-2017 рр.) Яковлєв С.В. працював на кафедрі математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського. У фокусі його наукової уваги перебувають питання оцінювання доказової та практичної стійкості до диференціального, лінійного та інтегрального криптоаналізу та їх модифікацій, дослідження ARX-криптосистем, аналіз криптографічних примітивів до атак за побічними каналами.

Автором проведено ряд фундаментальних досліджень в галузі криптоаналізу блокових шифрів. Вперше одержано аналітичні оцінки стійкості немарковських алгоритмів шифрування до диференціального криптоаналізу для ряду загальних конструкцій блокових шифрів (фейстель-подібних схем, SP-мереж із різними уточненнями); зазначені оцінки обчислюються через певні параметри складових шифру – S-блоків та лінійних перетворень. Для ситуацій, коли одержання аналітичних оцінок неможливо, автор запропонував декілька алгоритмів обчислення оцінок стійкості шляхом формалізованих розрахунків та запропонував загальну методику оцінювання стійкості слово-орієнтованих блокових шифрів до диференціального криптоаналізу та аналізу неможливих диференціалів. Результати, одержані по цьому напрямку, були використані для оцінювання стійкості нового національного стандарту шифрування ДСТУ 7624:2014.

Також Яковлєв С.В. вперше запропонував атаку збоїв на національний стандарт шифрування ДСТУ ГОСТ 28147:2009 та дослідив її ефективність. Це дозволяє формулювати вимоги до надійних реалізацій даного шифру у спеціалізованих пристроях.

Одержані у наукових роботах результати Яковлєва С.В. дозволяють принципово підвищити рівень захищеності інформаційно-комунікаційних систем державних організацій і приватних підприємств, та є підґрунтям для подальшого розроблення складових елементів системи національної безпеки України у частині виявлення і протидії використання кібернетичної зброї.

Результати роботи впроваджено у практичну діяльність в Інституті кібернетики імені В.М. Глушкова НАН України, Національному банку України, Службі зовнішньої розвідки України, в навчальний процес кафедри математичних захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського, що підтверджується відповідними довідками та актами. Одержані наукові та практичні результати були використані при виконанні держбюджетних НДР, в яких автор був виконавцем та відповідальним виконавцем: «Дослідження стійкості і ефективності криптографічних алгоритмів захисту інформації та їх реалізацій з використанням додаткових даних» (шифр 2417-п, 2011-2012 рр.), держ. реєстр. № 0111U000342; «Сучасні методи аналізу і синтезу криптографічних алгоритмів та протоколів» (шифр 2618-п, 2013-2014 рр.), держ. реєстр. № 0113U000944; «Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень» (шифр 2830-п, 2015-2016 рр.), держ. реєстр. № 0115U000254; «Дослідження сучасних алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем і застосування цих методів до окремих систем криптографічного захисту інформації» (шифр «Горбуша», 2012-2013 рр.), держ. реєстр. № 0112U008392; «Дослідження сучасних алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем і застосування цих методів до окремих систем криптографічного захисту інформації» (шифр «Севрюга», 2013-2014 рр.), держ. реєстр. № 0113U005813; «Дослідження та застосування методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних» (шифр «Кета», 2014-2015 рр.), держ. реєстр. № 0114U004643; «Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації» (шифр «Мокрель», 2015-2016 рр.), держ. реєстр. № 0115U004118; «Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень» (шифр «Кобія», 2016-2017 рр.), держ. реєстр. № 0116U006384; «Дослідження, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем» (шифр «Аргус», 2017 р.), держ. реєстр. № 0117U001817.

Результати досліджень за темою роботи викладено у 27 наукових працях, з них: 5 статей у фахових наукових виданнях України з технічних наук, із них 1 – в співавторстві; 22 тез доповідей міжнародних та всеукраїнських наукових конференцій. Частка, виконана особисто претендентом у роботі, яка подається

на здобуття премії Президента України для молодих вчених, складає 33,3%. Враховуючи необхідність неухильного дотримання норм наукової етики, автор не використовує ідеї та напрацювання, які належать співавторам.

У виданнях, внесених до наукометричних баз DOAJ, DOI, Google Scholar, Index Copernicus, ROAD та інших, розміщено 16 публікацій. Загальна кількість посилань на публікації автора складає 9 (згідно з базою даних Google Scholar), h-індекс рівний 1.

Роботу «Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі» не було удостоєно державних нагород раніше.

Проректор з наукової роботи **М.Ю. Ільченко**

УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

03056, м. Київ, пр-т Перемоги, 37; тел. (+38 044) 204-82-82 тел./факс (+38 044) 204-97-88
http://www.kpi.ua e-mail: mail@kpi.ua ЄДРПОУ 02070921

_____ № _____
на № _____ від _____

Комітет з державних премій України
в галузі науки і техніки

ДОВІДКА

про творчий внесок кандидата технічних наук, доцента кафедри інформаційної безпеки Фізико-технічного інституту **Барановського Олексія Миколайовича** в роботі «**Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі**» для участі в конкурсі на здобуття Премії президента України для молодих вчених

Барановський Олексій Миколайович показав себе як перспективний молодий науковець, що займається розробкою методів інформаційних потоків. На момент виконання роботи (2012-2017 рр.) Барановський О.М. навчався у аспірантурі (2010-2015 рр.) та працював на кафедрі інформаційної безпеки (з 2010 р.) Фізико-технічного інституту НТУУ «КПІ ім. Ігоря Сікорського». Займається питаннями аналізу зовнішніх і внутрішніх інформаційних потоків, методами аналізу на основі теорії детермінованого хаосу, а також питаннями виявлення витоків інформації, розслідування інцидентів в інформаційних системах та аудиту безпеки інформаційних систем.

Барановським О.М. проведено низку фундаментальних досліджень в галузі аналізу інформаційних потоків, які стосуються використання методів теорії детермінованого хаосу таких, як фрактальний та вейвлет аналіз, а також метод рекурентних діаграз для визачення властивостей та прогнозування поведінки інформаційних потоків, зокрема мережевого трафіку. Для виявлення нетипової поведінки інформаційних потоків автором вперше запропоновано наступні критерії аналізу інформаційного потоку: міра рекурентності та детермінізму, довжина прихованих циклів, міра та час завмирання. Вони базуються на відновленні фазової траєкторії, аналізі рекурентних діаграм та обчисленні глибинних параметрів динаміки інформаційного потоку. За рахунок раціонального вибору параметрів реалізації методу рекурентних діаграм можна більш ефективно виявляти зміни в динаміці інформаційних потоків.

Для оцінки коректності та швидкості розрахунку методами фрактального аналізу параметрів часових рядів інформаційних потоків з великими обсягами вхідних даних Барановським О.М. був удосконалений метод моделювання

фрактального броунівського руху. Це дає змогу, в залежності від особливостей інформаційного потоку, вибрати найбільш ефективний метод його фрактального аналізу.

Барановським О.М. розроблено інформаційну технологію дослідження інформаційних потоків, яка дозволяє зменшити час виявлення особливої поведінки інформаційних потоків.

Результати наукових праць Барановського О.М. дозволяють принципово підвищити рівень захищеності інформаційно-комунікаційних систем державних організацій і приватних підприємств, об'єктів критичної інфраструктури шляхом виявлення витоків в стандартних каналах комунікації. Результати можуть бути використані для подальшого розроблення складових елементів системи національної безпеки України у частині виявлення і протидії використання кібернетичної зброї.

Результати роботи впроваджено у практичну діяльність в навчальний процес кафедри інформаційної безпеки Фізико-технічного інституту НТУУ «КПІ ім. Ігоря Сікорського», що підтверджується відповідними довідками та актами. Одержані наукові та практичні результати були використані при виконанні держбюджетних НДР, в яких автор був виконавцем: №0113U002468 «Логіко-ймовірнисний підхід в задачах безпеки структурно-складних систем», №0113U007101 «Дослідження та розроблення методів відновлення фрагментів телекомунікаційних мереж та пошуку і аналізу їх параметрів.» шифр «Лазурит».

Результати досліджень за темою роботи викладено у 11 наукових працях, з них: 2 статі у фахових наукових виданнях України з технічних наук, із них 1 – в співавторстві; 4 статті у зарубіжних наукових виданнях з технічних наук, із них 2 – у співавторстві; 5 тез доповідей міжнародних та всеукраїнських наукових конференцій. Частка, виконана особисто претендентом у роботі, яка подається на здобуття премії Президента України для молодих вчених, складає 33,3%. Враховуючи необхідність неухильного дотримання норм наукової етики, автор не використовує ідеї та напрацювання, які належать співавторам.

У виданнях, внесених до наукометричних баз DOAJ, DOI, Google Scholar, Index Copernicus, ROAD та інших, розміщено 8 публікацій. Загальна кількість посилань на публікації автора складає 14 (згідно з базою даних Google Scholar), h-індекс рівний 2.

Роботу «Комплекс протидії витоку інформації з обмеженим доступом у критичній інформаційній інфраструктурі » не було удостоєно державних нагород раніше.

Проректор з наукової роботи **М.Ю. Ільченко**