ВІДГУК

офіційного опонента на дисертаційну роботу
Складанного Павла Миколайовича
«Моделі і методи забезпечення імітостійкості та конфіденційності
в системах обробки інформації»,
представлену на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – інформаційні технології

Відгук підготовлено за матеріалами дисертаційної роботи загальним обсягом 150 сторінок. Основний зміст роботи викладено на 130 сторінках дисертації, у тому числі в 14 таблицях та 25 рисунках, на 24 сторінках автореферату та у 21 науковій праці здобувача. Результати дисертаційного дослідження впроваджено, як у наукових установах НАН України, так й у закладах вищої освіти та науково-виробничих підприємствах нашої держави, що підтверджено 3 Актами впровадження.

1. Актуальність теми дисертаційної роботи

Розвиток сучасних інформаційних технологій та впровадження комп'ютерних систем в усі сфери людської діяльності стали причиною різкого зросту інтересу широкого кола користувачів до проблеми інформаційного захисту. Серед спектру методів захисту інформації особливе місце займають криптографічні методи. На відміну від інших, ці методи спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її оброблення, передавання і зберігання.

Постійне зростання інтересу до криптографії викликане останнім часом широким використанням і постійним збільшення об'єму інформаційних потоків. Проблему їх захисту можна вирішити як за рахунок застосування програмних криптографічних засобів, які не потребують великих фінансових витрат, так і апаратних криптосистем. Це гарантує надійний захист, але й разом з тим супроводжується імовірністю знаходження нових методів криптоаналізу, які дозволять послабити стійкість криптоалгоритмів.

Такий стан справ обумовлює, в свою чергу, цілу низку задач, що передбачають, зокрема, створення нових та удосконалення існуючих методів виявлення атак на програмні реалізації, методів забезпечення імітостійкості та оцінки ефективності застосування криптосистем. Вирішення поставлених задач дозволить створити нові методи і моделі криптозахисту, основними перевагами яких будуть високий рівень імітостійкості, зменшена вартість та значно збільшена швидкість часу виявлення атак, а також вдосконалити існуючі. Саме з цього й випливають задачі наукового обґрунтування можливості підвищення рівня імітостійкості та конфіденційності

інформації в системах обробки інформації в умовах кібератак. Тема досліджень дисертації, що розглядається, відповідає державній Стратегії кібербезпеки України. Робота виконувалась за напрямками наукових досліджень Інституту телекомунікацій та глобального інформаційного простору НАН України та кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи П.М.Складанного та наукову новизну поставлених в ній завдань дослідження.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення рівня імітостійкості та конфіденційності інформації в системах обробки інформації в умовах кібератак, за рахунок розробки й впровадження адекватних умовам застосування методів і моделей забезпечення надійного криптозахисту таких систем. Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, основними науковими результатами дисертації можна вважати:

- вперше розроблений метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в системах обробки інформації, шляхом реалізації двоступеневого критерію виявлення аномалій, що забезпечило можливість своєчасного виявлення моменту настання певної критичної ситуації та прийняття рішення щодо подальших дій;
- вперше розроблену модель функціонування шифратора багато алфавітної заміни для модуля криптографічного захисту інформації, впровадження якої за рахунок методу виявлення атак на програмні реалізації засобів криптографічного захисту інформації та методу генерації потоку підстановок дозволяє забезпечити конфіденційність і цілісність інформації, та підвищити функціональну безпеку та живучість самої системи в умовах кібератак;
- вперше розроблений метод генерації потоку підстановок шифру багатоалфавітної заміни шляхом реалізації імітостійкого шифрування на основі запропонованого швидкісного алгоритму формування потоку підстановок замін, а також критерію вибору степеню таких замін та процедури оцінки якості послідовності підстановок, що забезпечило необхідну швидкість криптоперетворення та захист повідомлень від підробки;
- удосконалений метод оцінки ефективності застосування криптосистем, на основі врахування співвідношення середнього значення максимальних втрат власника системи обробки інформації у випадку успішних кібератак до

мінімальної вартості реалізації таких атак, що дозволило, на відміну від існуючих, визначити границі відносної ефективності системи захисту інформації.

3. Достовірність наукових результатів

Точність та достовірність одержаних в роботі результатів підтверджується збігом результатів теоретичних досліджень з результатами імітаційного моделювання, а також збіжністю отриманих результатів з відомими частковими рішеннями.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної задачі в теорії побудови комп'ютерних криптографічних засобів надійного захисту інформації з високою швидкістю шифрування, для систем обробки інформації функціонуючих в умовах кібератак. Змістовний аспект запропонованого рішення, який спрямований на підвищення рівня імітостійкості та конфіденційності інформації в системах обробки інформації в умовах кібератак, за рахунок розробки й впровадження адекватних умовам застосування методів і моделей забезпечення надійного криптозахисту таких систем, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби забезпечення імітостійкості та конфіденційності інформації в системах обробки інформації в умовах кібератак. Результати роботи впроваджено в Національному центрі управління та випробувань космічних засобів, Інституті проблем математичних машин і систем НАН України та в навчальний процес Київського університету імені Бориса Грінченка.

6. Структура роботи

Дисертаційна робота містить вступ, 3 розділи, переліки використаних джерел по розділах, висновки та додатки.

У вступі обґрунтовано актуальність теми роботи, сформульовано мету і задачі дослідження, описано наукову новизну та практичне значення отриманих результатів, показано зв'язок роботи з науковими програмами, планами і темами, виконуваними у Київському університеті імені Бориса Грінченка Міністерства освіти і науки України, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

У першому розділі проведено аналіз сучасного стану проблем забезпечення імітостійкості та конфіденційності в системах обробки інформації, зокрема, проаналізовано множину актуальних загроз та уразливостей систем обробки інформації, розглянуто шляхи забезпечення імітостійкості та конфіденційності програмних засобів криптографічного захисту інформації. Досліджено методи та механізми забезпечення криптографічного захисту даних від спроб підробки інформації. Наведено способи реалізації засобів криптографічного захисту інформації. Описано обґрунтування необхідності розробки нових та удосконалення існуючих методів та моделей для забезпечення імітостійкості та конфіденційної даних в системах обробки інформації Сформульовано мету та задачі дослідження.

Другий розділ присвячено розробці моделей та методів забезпечення імітостійкості та конфіденційності в системах обробки інформації, а саме методу генерації потоку підстановок з використанням шифру багатоалфавітної заміни для забезпечення імітостійкого шифрування в системах обробки інформації, який включає в себе алгоритм генерації потоку підстановок для шифру багатоалфавітної заміни, алгоритму вибору степеню підстановок та процедуру перевірки послідовностей підстановок та оцінки їх якості. Метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в системах обробки інформації, який складеться з процедури виявлення прихованих каналів та моделі виявлення атак на програмні реалізації засобів криптографічного захисту інформації. На основі розроблених методів було побудовано модель функціонування шифратора багатоалфавітної заміни (модуля криптографічного захисту інформації) в системах обробки інформації котра дозволила створити цілісну картину представлення наукових результатів.

Третій розділ присвячено експериментальним дослідженням, що проводились шляхом імітаційного моделювання, а також виробленню рекомендацій щодо практичного застосування розроблених методів та моделей, на прикладі дистанційно пілотованих літальних апаратів. Для цього, зокрема, здобувачем було створено макет моделюючого комплексу інформаційної технології криптографічної обробки інформації, результати апробації якого підтвердили дієздатність та ефективність розроблених моделей та методів. Також у розділі подано удосконалений метод оцінки ефективності застосування криптосистем.

У додатках подано акти впровадження результатів дисертаційного дослідження, лістинг програми генерації потоку підстановок шифру багатоалфавітної заміни та обов'язковий додаток щодо апробації результатів.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методів і моделей для підвищення імітостійкості та конфіденційності інформації в системах обробки

інформації при кібератаках достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях і семінарах.

8. Автореферат дисертації

Автореферат за своїм змістом повністю відповідає дисертаційній роботі.

9. Зауваження щодо змісту дисертаційної роботи та автореферату

1. У першому розділі під час аналізу автоматизованих систем обробки інформації здобувач, на мій погляд, досить однобоко розглядає їх сучасний стан. Розгляд СОІ з позицій Закону України «Про основні засади забезпечення кібербезпеки України» певним чином звужує рамки дослідження, залишаючи при цьому поза увагою питання захисту інформації, що становить державну таємницю. Разом з тим, розділ 1 дисертації перевантажений загальними положеннями та визначеннями, які в подальшому не використовуються (наприклад, ст. 26, 29-31, 35).

2. У розділі 2 дисертаційної роботи алгоритм вибору степеня підстановок/замін шифру БАЗ для забезпечення захисту повідомлень від підробки було б доцільно подати у вигляді блок-схеми, а діаграму послідовності дій порушника в ході кібератаки (рис.2.5, ст.70) ототожнити як зі специфікою кібератаки, так і з рівнями можливостей порушника в ході кібератаки, які представлені на рис.2.6.

3. У розділі 2 дисертаційної роботи модель функціонування шифратора багатоалфавітної заміни (підрозділ 2.3) наведено без додаткових пояснень та прикладу шифрування-розшифрування, що певним чином ускладнює її сприйняття.

4. Особливості застосування дистанційно пілотованих літальних апаратів для моніторингу периметру контрольованої зони, що наведені в 3 розділі (ст. 96-99), а також опис статистичних тестів NICT_STS [108-112] можна винести в додатки.

5. У розділі 3 дисертаційної роботи результати обчислення часу на виконання задач зашифрування/розшифрування інформації, отримані при застосуванні створеної швидкодіючої криптосхеми (ст. 104) прив'язані до конкретної технічної реалізації і не показують переваги в порівнянні з іншими криптоалгоритмами.

6. Запропонований в роботі метод оцінки ефективності застосування криптосистем в СОІ є інтуїтивно зрозумілим, але було б доцільно подати його покрокову реалізацію та приклад його застосування.

7. Тексти дисертації та автореферату містять велику кількість скорочень та абревіатур, що певною мірою ускладнює загальний процес розуміння та оцінки результатів роботи. В дисертації та авторефераті присутні граматичні та стилістичні помилки.

Проте, зазначені недоліки не знижують ступінь наукової новизни та практичного значення одержаних в дисертації наукових результатів і, відповідно, позитивну оцінку роботи у цілому.

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення рівня імітостійкості та конфіденційності інформації в системах обробки інформації в умовах кібератак, за рахунок розробки й впровадження адекватних умовам застосування методів і моделей забезпечення надійного криптозахисту таких систем.

Дисертація є завершеною науково-дослідною роботою.

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики, дисертаційна робота задовольняє вимогам п.п 9, 11, 12, 13 "Порядку присудження наукових ступенів", затвердженого постановою КМУ №567 від 24.07.2013 р. (зі змінами, внесеними згідно з Постановами КМУ №656 від 19.08.2015., №1159 від 30.12.2015 р., та №567 від 27.07.2016 р.), а її автор Складанний Павло Миколайович заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 –інформаційні технології.

Офіційний опонент

завідувач кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету,
доктор технічних наук, професор

В.М. Рудницький

Учений секретар
к.т.н., доцент

Т.В. Шевченко