Голові спеціалізованої вченої ради Д 26.255.01
Інститут телекомунікацій і глобального
інформаційного простору НАН України

03186, м. Київ, бул. Чоколівський, 13

ВІДГУК

офіційного опонента – завідувача кафедри інженерії програмного забезпечення факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету доктора технічних наук, доцента Зибіна Сергія Вікторовича на дисертаційну роботу Складанного Павла Миколайовича на тему: "Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації", подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 - інформаційні технології

Актуальність теми дисертації

У теперішній час практично всі підприємства використовують автоматизовані системи обробки інформації для підвищення виробничих показників та прийняття більш зважених рішень. Чим складніша та функціональніша система, тим більше вразливих місць з точки зору кібератак. Однак досить складно забезпечити безпеку подібних систем через велику кількість вразливостей у них. При цьому загрози можуть надходити як із зовнішнього периметру, так і внутрішнього оточення, тому забезпечення безпеки інформаційних систем являється однією з пріоритетних проблем в сучасному середовищі.

Тому дослідження, що спрямовані на розроблення ґрунтовних засад побудови теоретичних і прикладних засад побудови та забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в системах обробки інформації з урахуванням множини кіберзагроз та потенційно можливих наслідків їх реалізації являється **актуальними**.

Значення дисертації для науки й практики

Наукова новизна одержаних результатів визначається наступним:

1. Вперше розроблений метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в системах обробки

інформації(СОІ), впровадження якого шляхом реалізації двоступеневого критерію виявлення аномалій дозволяє своєчасно виявити момент настання певної критичної ситуації та прийняти рішення щодо подальших дій.

2. Вперше розроблена модель функціонування (криптосхема) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ, впровадження якої за рахунок метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ та методу генерації потоку підстановок для шифру БАЗ дозволяє забезпечити конфіденційність і цілісність інформації, що циркулює в СОІ, та в умовах кібератак підвищити функціональну безпеку та живучість самої системи.

3. Вперше розроблений метод генерації потоку підстановок шифру багатоалфавітної заміни для забезпечення в СОІ конфіденційності та цілісності інформації, впровадження якого за рахунок реалізації імітостійкого шифрування на основі оригінального швидкісного алгоритму формування потоку підстановок замін, критерію вибору степеню таких замін та процедури оцінки якості послідовності підстановок шифру багатоалфавітної заміни дозволяє обрати таку степінь підстановок, яка б забезпечувала достатню швидкодію криптоперетворення та була б раціональною для забезпечення захисту повідомлень від підробки.

4. Удосконалений метод оцінки ефективності застосування криптосистем, на базі врахування співвідношення середнього значення максимальних втрат власника СОІ у випадку успішних кібератак на систему захисту до мінімальної вартості реалізації таких атак, що дозволило, на відміну від існуючих, визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах реалізації кіберзагроз.

Практичне значення сукупності складає підґрунтя для забезпечення імітостійкості та конфіденційності каналів передачі даних (команд управління) в СОІ..

Практична цінність дисертаційної роботи полягає у тому, що отримані результати дозволяють:

1. визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах кібератак;

2. знизити ймовірність підробки команди управління до прийнятної для практичного застосування величини, що оцінується величиною 10^{-6};

3. знизити час на виявлення атаки приблизно на 20%;

4. знизити вартість системи виявлення атак на програмні реалізації засобів КЗІ приблизно на 25%.

Практична цінність роботи, також, підтверджується актами впровадження основних результатів дослідження, що додаються до дисертаційної роботи.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їхня достовірність і новизна

Обґрунтованість наукових результатів, висновків та рекомендацій забезпечена коректним використанням апробованого математичного апарату, повнотою врахування початкових даних та визначенням і дотриманням доцільних обмежень та припущень.

Достовірність наукових положень підтверджена результатами апробації процедур, які було розроблено у процесі створення моделе та методів забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в СОІ.

Висновки та рекомендації щодо наукового та практичного використання здобутих результатів

Результати дисертаційної роботи доцільно використовувати в науково-дослідних інститутах і конструкторських бюро для створення або удосконалення існуючих систем обробки інформації з метою забезпечення надійного криптозахисту таких систем.

Повнота викладу в опублікованих працях

Основні положення та результати дисертаційної роботи достатньо повно опубліковані у 21 науковій праці, 1 колективна монографія, 9 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України, 3 наукові праці, що входять до наукометричної бази SCOPUS. Разом з тим основні наукові результати додатково відображені у 9 тезах доповідей на семінарах та науково-практичних конференціях.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

За своїм змістом дисертація Складанного П.М. відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня кандидата наук і являє собою наукову працю, яка містить сукупність наукових положень та результатів, виставлених автором для публічного захисту, має внутрішню єдність і свідчить про особистий внесок автора у науку.

Оформлення дисертації та автореферату відповідає вимогам Державних стандартів України. Текст дисертації та автореферату написані грамотною технічною мовою, ясно та зрозуміло.

У ***вступі*** обґрунтовано актуальність теми дисертації, сформульовано мету, об'єкт, предмет, завдання дослідження, наукову новизну одержаних

результатів, практичне значення результатів, зв'язок роботи з науковими програмами, планами та темами досліджень. Визначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації.

У ***першому розділі*** дисертації: проаналізовано стан проблеми забезпечення імістостійкості та конфіденційності СОІ; проаналізовано загрози та уразливості, що впливають на дієздатність СОІ; досліджено фактори що сприяють реалізації атак на СОІ, шляхи забезпечення імітостійкості та конфіденційності програмних реалізацій засобів КЗІ, методи та механізми криптографічного захисту даних, а також розглянуті особливості та способи реалізації засобів криптографічного захисту інформації.

У ***другому розділі*** дисертації запропоновано метод генерації потоку підстановок для шифру багатоалфавітної заміни (БАЗ).

Розглянуто алгоритми та процедури, які входять до запропонованого методу: швидкісний алгоритм генерації потоку підстановок для шифру багатоалфавітної заміни; алгоритм вибору степеню підстановок/замін шифру БАЗ для забезпечення захисту повідомлень від підробки; процедура перевірки послідовності підстановок шифру багатоалфавітної заміни та оцінки їх якості.

У ході реалізації другого розділу дисертаційної роботи запропоновано методу виявлення атак на програмні реалізації засобів КЗІ в СОІ.

Розглянуто: шляхи забезпечення цілісності програмних реалізацій засобів криптографічного захисту інформації; запропоновано уточнену модель порушника і загроз в СОІ, а також автоматну модель безпеки функціонування каналів управління системи; процедуру виявлення прихованих каналів в ході атак на програмну реалізацію стійких криптографічних алгоритмів.

Запропоновано модель функціонування (криптосхема) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ побудована за рахунок метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ та методу генерації потоку підстановок для шифру БАЗ.

У ***третьому розділі*** дисертації описано удосконалений метод оцінки ефективності застосування криптосистем на базі врахування співвідношення середнього значення максимальних втрат власника СОІ у випадку успішних кібератак на систему захисту до мінімальної вартості реалізації таких атак, що дозволило, на відміну від існуючих, визначити границі для відносної ефективності системи захисту інформації в СОІ в умовах реалізації кіберзагроз. Для практичної перевірки запропонованих у роботі методів та

моделей було створено макет моделюючого комплексу інформаційної технології криптографічної обробки інформації(МК ІТ КОІ).

У ході роботи МК ІТ КОІ біло проведено перевірку випадковості та рівномірності розподілу потоку підстановок, які утворювалися за допомогою генератора псевдовипадкових послідовностей. Подальшим кроком застосування МК ІТ КОІ проведено апробацію методу виявлення атак на програмні реалізації засобів КЗІ в СОІ

У висновках наводяться основні наукові та практичні результати.

Отже поставлені наукові завдання в повному обсязі вирішені та наведені в дисертаційній роботі. Вищенаведене дозволяє зробити висновок про відповідність назви дисертації її змісту.

Відповідність змісту автореферату основним положенням дисертації

Зміст автореферату повністю відображає основні результати досліджень, які подані в дисертації. В авторефераті в повній мірі викладені усі наукові положення та результати з достатньою детальністю.

Недоліки та зауваження

1. Не визначено, як зростатиме ймовірність вгадування порушником r символів за два і більше кроків. Такі ймовірності можуть бути порівняльними показниками при виборі методів захисту серед можливих, а також при визначенні необхідності застосування додаткових алгоритмів запобігання багатократних спроб. Це ж стосується і ймовірності підміни в каналі зв'язку істинного повідомлення на фіктивне.

2. У роботі не розглянуто вплив на показники системи з багатоалфавітною заміною (БАЗ) помилок, які виникають у каналі при передачі кодових комбінацій і які залишаються невиявленими та невиправленими навіть при застосуванні завадостійких кодів.

3.Зміна статистичних характеристик потоку вимірюваних даних від об'єкту може бути пов'язаний не тільки із діями порушника, а із зміною характеру джерел ненавмисних завад і з їх нестаціонарністю. Тому запропоновані модель та метод виявлення атак на основі контролю математичного сподівання не є досконалими і потребують подальших досліджень.

4. Розмір приведених в дисертації та авторефераті зображень (таблиць і рисунків) ускладнює ознайомлення з текстовою інформацією, що в них відображена. Даний недолік притаманний тільки паперовій копії. В електронному варіанті рисунки і таблиці піддаються масштабуванню.

5. Не надані результати оцінювання величин показників кількості підстановок, що генеруються; ймовірності їх зустрічальності та матриці перехідних ймовірностей у порівнянні з іншими методами.

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

Висновки

Дисертаційна робота Складанного Павла Миколайовича є завершеною актуальною науковою працею, що має значну наукову та практичну цінність у розробленні теоретичних і прикладних засад побудови та забезпечення методами криптографічної обробки інформації імітостійкості та конфіденційності даних в СОІ з урахуванням множини кіберзагроз та потенційно можливих наслідків їх реалізації.

За глибиною теоретичного обґрунтування та практичної значущості дисертація відповідає 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 за спеціальністю 05.13.06 - інформаційні технології.

Офіційний опонент
завідувач кафедри інженерії
програмного забезпечення
факультету кібербезпеки,
комп'ютерної та програмної інженерії
Національного авіаційного університету
доктор технічних наук, доцент С.В. Зибін

«10» березня 2021 року

Підпис Зибіна С.В. засвідчую.

Начальник відділу кадрів
Національного авіаційного університету
(підпис)

Вчений секретар НАУ М. Лемський