Голові спеціалізованої вченої ради Д26.062.17
Національного авіаційного університету
03058, м. Київ, просп. Космонавта Комарова, 1

Відгук офіційного опонента

професора кафедри кібербезпеки та математичного моделювання
Національного університету "Чернігівська політехніка",
доктора технічних наук, професора Шелеста Михайла Євгеновича
на дисертацію Коваленка Богдана Анатолійовича
«Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах»,
поданої до захисту на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 – Системи захисту інформації.

Актуальність теми дисертації. Забезпечення інформаційної безпеки - глобальна задача, що лежить у сфері реалізації основних інтересів кожної держави, у тому числі, України. З огляду на широке використання криптографічних систем захисту інформації у інформаційно-телекомунікаційних системах, особливої гостроти набувають задачі захисту самих криптосистем на усіх етапах їх життєвого циклу. Однією з загроз щодо адекватного функціонування криптосистем є, зокрема, клептографічні атаки, мета яких – створення нападнику відповідних умов успішного відновлення ключів шифрування з подальшим дешифруванням криптографічно захищеної інформації.

Клептографія вивчає методи синтезу та аналізу каналів прихованого витоку секрету (embedded trapdoor, subliminal channel) на базі криптосистем, що дозволяє особі, яка впровадила такий канал, отримати певну чутливу інформацію. Клептографія є "рідною сестрою" криптографії та стеганографії, вони на протязі сторіччя щільно синхронно розвивалися.

Методи створення клептографічного нападу давно опановані спецслужбами. Особливого поширення вони зазнали у 70-х роках минулого сторіччя, коли на ринок стали масово постачатися спочатку електронні шифратори, а за ними програмні реалізації методів криптографічного захисту. З середини 90-х років XX-го сторіччя у відкритих наукових виданнях стали з'являться перші результати досліджень щодо клептографічних проблем.

Можливими напрямками вирішення проблеми захисту криптосистем від клептографічних атак є створення наукової бази щодо розробки методів оцінки наявності клепрографічних загроз; побудова відповідних методів виявлення та протидії таким загрозам; синтез криптографічних систем та криптопримітивів з клепто закладками, тощо.

Проте методи захисту від клептографічних атак наразі зводяться до традиційного криптоаналізу потенційно вразливих систем, до певних інтуїтивних рекомендацій (яких далеко не завжди дотримуються) відносно процесу розробки базових заходів захисту програмно-апаратних засобів. Відсутність системного підходу до побудови криптосистем, що є стійкими до клептографічних атак та методів оцінки наявності клепто закладок призводить до ризиків інформаційної безпеки, які підвищуються з ростом розповсюдженості криптосистем та довіри до розробника криптосистеми.

Таким чином, актуальними є задачі створення методів побудови криптосистем та криптопримітивів з доведеної стійкістю до клептографічних атак, а також створення науково обґрунтованих підходів до оцінки ризиків наявності клепто закладок у примітивах на етапі розробки та відбору до використання. Вирішенню деяких з цих задач і присвячене надане дисертаційне дослідження.

Загальна характеристика дисертаційної роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел з 90 найменувань та додатків. Зміст та структура роботи у повній мірі відповідають завданню з викладення основних результатів для досягнення поставленої в дослідженні мети та сформульованим задачам, що відповідають паспорту спеціальності 05.13.21 – Системи захисту інформації.

Перший розділ присвячено аналізу сучасного стану клептографічних досліджень. Введено неформально поняття клептографічного механізму як розширення поняття криптосистеми з додатковою функцією Розробника, та проведено порівняння з можливостями клептографії та стеганографії. Продемонстровано найвідоміші криптопримітиви із можливими вбудованими клепто закладками, зокрема: алгоритм симетричного шифрування DES, генератор псевдовипадкових послідовностей DualEC DRGB, потенційні закладки у російських стандартах гешування (ГОСТ Р 34.11-2012) та шифрування (ГОСТ Р 34.12-2015), закладки у структурі еліптичної кривої та канали витоку секрету на базі клептографічного механізму SETUP авторів Янга і Юнга для протоколів на базі дискретного логарифмування та факторизації.

У результаті проведеного у розділі аналізу сформульовано основні задачі та проблеми клептографії.

Другий розділ присвячено розробці теоретичних положень захисту криптосистем від клептографічних атак. Показана неадекватність існуючих моделей криптографічної стійкості для оцінки стійкості клептографічних механізмів. Введено поняття практичної нерозрізненості алгоритмів (на противагу поліноміальній нерозрізненості). Автор використовує поняття практичної нерозрізненості для формалізації клептографічної лазівки, оскільки вона є практично односторонньою функцією, що загалом не підпадає під модель теоретико-інформаційної чи обчислювальної складності. Запропоновано статистичну модель розподілу інформації криптопротоколу та створено загальну класифікацію клептографічних механізмів.

Запропоновано формальну модель базового протоколу "запит-відповідь" із клептографічним каналом витоку та доведено теорему про необхідну умову наявності каналу витоку. На базі цього розроблено *метод побудови (модифікації) криптопротоколів з доведенням відсутності клептографічного каналу витоку секрету*.

Введено поняття клептографічного потенціалу як міри потенціальної наявності клептографічної закладки у криптопримітиві. Оцінка клептографіічного потенціалу на практиці є складною задачею, оскільки обмеження на множини допустимих та заборонених функцій найчастіше є нетривіальними. Більш того, в ряді випадків необхідно ще оцінювати клептографічні ризики для уже існуючих криптопримітивів, це ускладнює задачу визначення множини допустимих функцій. Тому автор для більшої практичності вводить поняття «клептографічної надлишковості».

В роботі наведено базові правила, що можуть визначати відношення еквівалентності криптопримітивів, та розроблено базову схема процесу зменшення клептографічних ризиків гібридної криптосистеми. Компонентами такої схеми є база відомих клептографічних механізмів, база відомих криптографічних примітивів та протоколів та власне цільова гібридна криптосистема.

У третьому розділі на базі вказаного вище методу наведено приклади застосування клептографічних методів для побудови криптосистем з каналами витоку та з доведеною їх відсутністю. Зокрема, запропоновано модифікацію базового протоколу запиту унікальної послідовності nonce та формально доведено відсутність можливості створення непомітного каналу витоку секрету на його основі. Також запропоновано модифікацію протоколу узгодження ключа Діффі-Хеллмана, що є стійкою до атаки Янга та Юнга,

формально доведено відсутність можливості створення непомітного каналу витоку секрету під час роботи протоколу. Ключовим принципом роботи цих методів є те, що жоден з абонентів системи не використовує в протоколах внутрішні джерела випадковості, а усі псевдовипадкові послідовності генеруються на базі публічних унікальних значень з механізмами доведення оригінальності (відсутності модифікацій). Це дозволяє забезпечити виконання достатніх умов про відсутність каналу непомітного витоку секрету.

Продемонстровано можливість побудови геш функції на базі конструкції Меркла-Дамгарда із вбудованим клептографічним механізмом, що дозволяє Розробнику, який знає секрет у структурі примітиву, ефективно знаходити прообраз. Продемонстрована потенціальна можливість використовувати геш функції з набором таємних диференційних шляхів високої ймовірності для отримання переваги Розробником у системі технології розподіленого реєстру блокчейн.

У четвертому розділі проводиться аналіз ефективності методу побудови блокчейн системи з Proof-of-Work алгоритмом консенсусу із закладкою для різних початкових умов. Отримано практичні оцінки ефективності деяких клептографічних атак та методів клептографічного аналізу. Зокрема, для лазівки у блокчейн протоколах консенсусу Proof-of-Work отримано оцінки переваги Розробника для різної кількості контрольованих бітів та ймовірності допоміжних диференційних шляхів. Наприклад, у випадку контролю лише одного біта, перевага Розробника може сягати 50%.

Також для ряду примітивів (геш-функцій та алгоритмів симетричного шифрування) були отримано оцінки клептографічної надлишковості. Розрахунки показали, що серед розглянутих алгоритмів найбільша клептографічна надлишковість у російському стандарті геш функції ГОСТ Р-34.11-2012 – 12582.19 біт (тобто за даною метрикою, алгоритм має найбільший ризик містити клептографічний механізм). Натомість, найменша клептографічна надлишковість спостерігається в стандарті блокового шифрування AES – 32.

Висновки дисертаційної роботи підкреслюють наукову новизну та практичну цінність проведених досліджень. Основні результати мають як теоретичну, так і практичну складову, створюючи у сукупності можливість підвищення рівня захищеності криптосистем від певного класу клептографічних атак.

Наукова новизна результатів, отриманих в дисертаційній роботі. Тема дисертаційної роботи безпосередньо пов’язана з напрямами наукових досліджень, сформульованими в пп. 1.2.1.1, 1.2.1.2, 1.2.7.1, 1.2.7.2 та 1.2.7.3

«Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», визначених постановою Президії НАН України від 20.12.13р. №179, стратегією кібербезпеки України від 15.03.16р. №96/2016.

Наукова та практична новизна отриманих у дисертаційній роботі результатів полягає у наступному:

1. *Вперше* запропоновано математичну модель для протоколів типу «запит-відповідь» у клептографічному сенсі, в результаті чого отримана можливість строгої оцінки клептографічної стійкості протоколів, що зводяться до протоколів типу «запит-відповідь».

2. *Вперше* отримано достатні умови неможливості непомітної клептографічної модифікації криптосистеми, у результаті чого з'явилася можливість строгого доведення відсутності клептографічної модифікації у криптографічних протоколах.

3. *Вперше* розроблено метод побудови функції гешування з клептографічним механізмом, в результаті чого можливе створення геш-функції з лазівкою, що дозволяє Розробнику частково відновлювати повідомлення за відомим геш-кодом.

4. *Вперше* запропонована метрика «клептографічного потенціалу», в результаті чого отримана можливість порівнювати клептографічні примітиви за ризиком наявності у них закладок.

5. *Вперше* запропоновано метод зменшення "клептографічного потенціалу" у криптопримітивах за допомогою генератора констант, в результаті чого мінімізуються ризики щодо наявності лазівки в криптопримітиві.

6. *Удосконалено* загальну класифікацію клептографічних систем Шнаєра, в результаті чого отримані вектори клептографічних атак на криптографічні системи та примітиви.

7. *Удосконалено* базові протоколи запиту nonce та узгодження ключа Діффі-Хеллмана, в результаті чого отримана база для побудови 106 криптографічних протоколів зі строго доведеною відсутністю клептографічного каналу витоку.

8. *Здійснено подальший розвиток* методу Пренеля побудови шифру для побудови клептографічної функції гешування, в результаті чого, у випадку використання такої функції у блокчейн протоколах консенсусу Proof-of-Work перевага Розробника підвищується до 50% порівняно зі звичайним учасником. Для даного випадку отримано оцінки переваги Розробника для різної кількості контрольованих бітів та ймовірності допоміжних диференційних шляхів.

9. *Отримано чисельні значення клептографічної надлишковості* для відомих криптопримітивів (геш функцій та алгоритмів симетричного шифрування). Наприклад, розрахунки показали, що серед розглянутих алгоритмів найбільша клептографічна надлишковість у російського стандарту геш функції ГОСТ Р-34.11-2012 – *12582* біт (тобто за даною метрикою, алгоритм має найбільший ризик містити клептографічний механізм). Натомість, найменша клептографічна надлишковість спостерігається в стандарті блокового шифрування AES – *32*, тобто клептографічний потенціал AES можна зменшити на 32 біти.

Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій, сформульованих у дисертації, визначається наступним:

- теоретичні дослідження базуються на фундаментальних положеннях і не суперечать відомим науковим фактам;
- теоретичні результати обґрунтовані коректним використанням математичного апарату – абстрактної та лінійної алгебри, математичної логіки, теорії алгоритмів та теорії складності обчислень, теоретичних основ криптографії;
- коректністю поставлених задач при проведенні експериментальної перевірки отриманих теоретичних результатів;
- відповідністю результатів експериментів теоретичним положенням, набутим при проведенні дисертаційного дослідження.

Практичне значення результатів, отриманих в дисертаційній роботі, полягає в доведенні здобувачем отриманих наукових результатів до конкретних алгоритмів та програмних реалізацій, що можуть бути використані як для підвищення рівня захищеності криптосистем при часткової компрометації одного з учасників, так й для створення можливих лазівок у криптосистемах і криптопротоколах на базі розроблених клепрографічних механізмів.

Робота виконана в рамках науково-дослідної роботи «Корифена» (державний номер реєстрації 0118U001653) на замовлення Служби зовнішньої розвідки України, науково-дослідної роботи «Родоліт» (державний номер реєстрації 011U007473) на замовлення Служби безпеки України та згідно з планами науково-дослідної роботи Фізико-технічного інституту КПІ ім. І. Сікорського, в яких автор був виконавцем.

Практичне значення отриманих результатів підтверджене актами впровадження у діяльності Національного банку України та військової частини Р9000 Служби безпеки України.

Повнота викладення наукових положень, висновків та рекомендацій, сформульованих у дисертаційному дослідженні та опублікованих у працях. Результати дисертаційного дослідження знайшли своє відображення в 7 наукових роботах, у тому числі: 1 науковій статті у науково періодичному виданні, що входить до наукометричної бази SCOPUS; 5 статей в журналах, що включено до Переліку фахових видань України; 1 статті у електронному журналі IACR, що видається Міжнародною асоціацією криптографічних досліджень. Усього одноосібних статей – 1. Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації як на вітчизняному, так і на міжнародному рівнях.

Наукові результати, отримані у дисертаційному дослідженні, доповідалися і обговорювалися на 4 міжнародних та всеукраїнських науково-практичних конференціях, а також наукових семінарах при Вченій раді НАН України, зокрема "Проблеми сучасної криптології" та "Методи обчислювальної математики та математичне моделювання процесів в неоднорідних середовищах". матеріали дисертації доповідалися і обговорювалися на 4 міжнародних та всеукраїнських конференціях, де отримали позитивну оцінку провідних фахівців-криптологів та науковців у галузі захисту інформації.

Зауваження дисертаційної роботи та автореферату.

1. Підхід до побудови протоколів без лазівки у розділі 3.1 передбачає використання підпису публічних, але унікальних послідовностей. Проте, якщо ми говоримо про практичні протоколи, то потрібно враховувати можливості компрометації, в результаті якої зловмисник здатний відновити всі попередні значення генератора (тобто протокол не задовольняє вимогам прямої безпеки forward secrecy).

2. Під час визначення клептографічної надлишковості передбачається, що алгоритм знаходиться у процесі розробки і аналітик порівнює надлишковість готового алгоритму відносно попередньо заданої структури. Тому не зрозуміло, як це працює при оцінці потенціалу для існуючих криптопримітивів.

3. У розділі 4.2 надлишковість рахується за певними параметрами (наприклад, константами), але не враховує інші параметри (наприклад, кількість раундів, розмір блоку повідомлень, тощо). Чим аргументується такий критерій вибору параметрів для оцінки?

Проте зазначені недоліки не знижують наукової та практичної значимості результатів, отриманих автором у процесі виконання роботи.

Більш того, отримані результати дають автору можливість у подальшому розвинути подальші дослідження за наступними напрямками:

1. Побудови лазівок в криптоалгоритмах без використання готових асиметричних примітивів.
2. Розвиток означеної в роботі ідеї щодо оцінки клептографічного потенціалу протоколів.
3. Побудови інших видів протоколів без витоку секрету, які не є протоколами типу "запит-відповідь" (особливо протоколи з трьома та більше абонентами).

Відповідність дисертації встановленим вимогам і загальні висновки. Дисертаційна робота Коваленко Богдана Анатолійовича на тему «Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах» є завершеним науковим дослідженням.

В роботі вирішено ряд важливих наукових та науково-практичних задач щодо підвищення рівня захищеності гібридних криптосистем проти клептографічних атак. Представлені на захист наукові положення розроблено автором самостійно. *Аналогічних рішень в Україні та закордоном немає, що робить результати досліджень пріоритетними.*

Дисертація відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації.

Автореферат дисертації об'єктивно і достатньо повно відображає зміст, а також основні положення та висновки дисертації.

Матеріали дисертації опубліковано у 7 наукових працях (одна з яких – одноосібна). Наукові результати та положення дисертаційної роботи пройшли опробування на 4 міжнародних та всеукраїнських конференціях, а також на семінарах НАН України.

Аналізуючи надану дисертаційну роботу, можна зробити висновок про те, що дисертаційна робота Коваленко Богдана Анатолійовича на тему «Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах» є самостійно виконаним завершеним дослідженням, в якому *отримано нові суттєві науково обґрунтовані результати*, що в сукупності вирішують поставлену мету роботи щодо забезпечення відповідного рівня захищеності криптосистем від клептографічних атак.

Розглянута дисертаційна робота відповідає вимогам п.п. 9-10, 12-13 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013р. №567 із змінами, внесеними згідно Постанови Кабінету Міністрів України №656 від 19.08.15 р., №1159 від

30.12.15р., №567 від 27.07.16 р., №943 від 20.11.19 р., а її **автор, Коваленко Богдан Анатолійович, заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації.**

Офіційний опонент
Заслужений діяч науки і техніки України,
Лауреат Державної премії України в галузі науки і техніки,
професор кафедри кібербезпеки та математичного моделювання
Національного університету "Чернігівська політехніка"

доктор технічних наук, професор М.Є. Шелест
"30" серпня 2020 року

Підпис Шелеста М.Є. засвідчую

Міністерство освіти і науки України * Національний університет "Чернігівська політехніка" * 05460798 *

Проректор
В. В. Ракульченко

"1" вересня 2020 року