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

Відгук офіційного опонента

доктора технічних наук, старшого наукового співробітника, начальника кафедри захисту інформації та кіберзахисту Військового інституту телекомунікації та інформатизації ім. Героїв Крут,
Чевардіна Владислава Євгенійовича
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. Криптографічні системи є критичним компонентом забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем та систем управління критичної інфраструктури держави. Поряд із задачами розробки квантовостійких криптографічних систем особливої гостроти набуває задачі алгоритмічної, програмних та програмно-апаратної реалізації криптографічних систем захисту інформації. С кожним десятиріччям арсенал умовного зловмисника доповнюється не лише новими методами криптоаналізу, квантовими комп'ютерами, а також можливістю втручатись в криптосистему на етапі розробки та реалізації. Прикладом такого втручання можна назвати створення лазівки в генераторі ПВП Dual_EC_DRBG, аналіз та вдосконалення якого було розглянуто в дисертаційних роботах вітчизняних вчених. Прискорення криптоаналізу системи зловмисником в умовах клептоатак викликало проблему розпізнавання лазівок на ранніх етапах реалізації криптосистеми та ефективної протидії ним, розкриття каналів прихованого витоку секрету (subliminal channel, kleptographic trapdoor), що стало предметом дослідження.

Таким чином, розробка науково обґрунтованих підходів до оцінки ризиків наявності клептозакладок у примітивах на етапі розробки та відбору до використання разом з темою роботи є актуальними.

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 огляду сучасних методів побудови клептомеханізмів та клептографічного аналізу, введені неформальні поняття клептографічного механізму на базу криптосистеми, де вводиться додаткова роль Розробника, наводяться порівняння із стеганографією та криптографією. Наводяться приклади відомих ймовірних клептографічних механізмів: 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), механізму SETUP для асиметричних криптосистем.

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

Другий розділ присвячено розробці теоретичних положень захисту криптосистем від клептографічних атак. В роботі вводиться поняття практичної нерозрізненості для формалізації клептографічної лазівки, оскільки аналіз її стійкості не підпадає під модель теоретико-інформаційної чи обчислювальної складності. Також пропонується статистична модель розподілу інформації криптопротоколу та загальна класифікація клептографічних механізмів.

Основним результатом роботи є формальна модель протоколу ”запит-відповідь”, який є базовим для багатьох криптографічних протоколів, та модель протоколу з клептографічним каналом витоку секрету.

У третьому розділі наведені приклади практичного використання раніше запропонованих підходів. Зокрема, пропонується модифікація базового протоколу генерації nonce та протоколу узгодження ключа Діффі-Хелмана на базі вказаного методу та доводиться відсутність каналу витоку секрету в них. Ідея роботи цих методів: жоден з абонентів системи не використовує в протоколах внутрішні джерела випадковості, а усі псевдовипадкові послідовності генеруються на базі публічних унікальних значень з подальшим

доведенням відсутності модифікацій. Це дозволяє забезпечити виконання достатніх умов про відсутність каналу непомітного витоку секрету.

Також продемонстровано можливість побудови геш функції на базі блокових шифрів та 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 підвищення рівня стійкості до гібридних криптосистем до певних класів 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 доведенною 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 досліджені, 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. В п. 2.7.1 дисертаційної роботи здобувач робить припущення, стосовно того, що окремі криптопримітиви, які можуть використовуватись під час розробки криптопротоколу, не містять клептографічних механізмів, але пізніше здійснює оцінку клептографічного потенціалу та клептографічної надлишковості для криптопримітиву, не уточнюючи для яких криптопримітивів це робить. Не зрозуміло також назву таблиці 1, а саме Клептографічна надлишковість різних симетричних клептографічних примітивів.

2. В дисертаційній роботі на стор.54 введено поняття клептографічного потенціалу, метрикою для якого вводить значення ϕ, яке також дає можливість

прогнозувати ризики наявності клептомеханізмів, та визначає головною метою дослідження – отримання метрики ϕ, яка є четвертим результатом, однак експериментальних чи підтверджуючих теоретичні оцінки значень не наводить, зокрема лише для клептографічної надлишковості (стор. 104, Таблиця 1).

3. Залишилось також за визначеними здобувачем рамками досліджень питання щодо значень клептографічної надлишковості криптопримітивів в жорстких умовах проведення конкурсів на міжнародний стандарт криптографічного захисту, наприклад симетричного шифрування – AES.

4. На рис. 2.5 наведено "Процес зменшення клептографічних ризиків гібридної криптосистеми", але в роботі не наводиться поняття клептографічного ризику та гібридної криптосистеми.

5. Деякі рисунки мають англійські абревіатури назв на графіках (рис. 4.1, 4.2.), але в тексті не вказано еквівалентного зв’язку з українською абревіатурою.

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.

Відповідність дисертації встановленим вимогам і загальні висновки. Дисертаційна робота Коваленка Богдана Анатолійовича на тему «Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах» є завершеним науковим дослідженням, в якої 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. Дисертація відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації. 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.

Відгук розглянутий на засіданні кафедри Захисту інформації та кіберзахисту Військового інституту телекомунікації та інформатизації ім. Героїв Крут, протокол №21 від 02.09.20.

Офіційний опонент

Начальник кафедри захисту інформації та кіберзахисту Військового інституту телекомунікації та інформатизації ім. Героїв Крут.

доктор технічних наук,
старший науковий співробітник
"02" вересня 2020 року

В. ЧЕВАРДІН

Підпис Чевардіна В.Є. засвідчую
"02" вересня 2020 року

ПІП-К С. ДИСЕНКО