DOI 10.25140/2411-5363-2023-3(33)-150-161
УДК 004.056

Юлія Ткач[1], Михайло Шелест[2], Марина Синенко[3], Тарас Петренко[4]

[1] доктор педагогічних наук, завідувач кафедри кібербезпеки та математичного моделювання національного університету «Чернігівська політехніка»
E-mail: tkachym79@gmail.com **ORCHID:** https://orcid.org/0000-0002-8565-0525
Scopus Author ID: 57193026076

[2] доктор технічних наук, професор кафедри кібербезпеки та математичного моделювання національного університету «Чернігівська політехніка»
E-mail: mishel3141@gmail.com **ORCHID:** https://orcid.org/0000-0003-1090-0371
Scopus Author ID: 57211429755

[3] кандидат фізико-математичних наук, доцент кафедри кібербезпеки та математичного моделювання національного університету «Чернігівська політехніка»
E-mail: mara.a.snnk@gmail.com **ORCHID:** https://orcid.org/0000-0002-8961-533X **Scopus Author ID:** 55884350800

[4] кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання національного університету «Чернігівська політехніка»
E-mail: 4650364@gmail.com **ORCHID:** https://orcid.org/0000-0001-5571-3815
Scopus Author ID: 57193026484

ІСТОРІЯ ВИНИКНЕННЯ КЛЕПТОГРАФІЇ ТА ЇЇ МІСЦЕ В БЕЗПЕЦІ ІНФОРМАЦІЇ

Актуальність теми дослідження. *Інформатизація суспільства породжує нові загрози: користувачами сучасних IT технологій стають не лише законослухняні громадяни, а й злочинці, шахраї чи терористи, які використовують їх для скоєння злочинів. Тому будь-яка держава намагається контролювати свій сегмент кіберпростору. Для вирішення такої задачі можуть знадобитися методи нової наукової дисципліни – клептографії.*

Постановка проблеми. *Для боротьби з тероризмом необхідно прийняти рішення на офіційному державному рівні про впровадження відповідного контролю інформаційних систем та мереж. А чи існують надійні способи забезпечення ексклюзивного доступу спецслужб до інформації користувача при збереженні достатнього рівня стійкості до сторонніх зловмисників? Ці питання вирішує клептографія.*

Аналіз останніх досліджень і публікацій. *Сучасні дослідження з клептографії, окрім класичних робіт, де впроваджено базові поняття та терміни, в основному присвячені виключно синтезу криптосистем із закладкам. Проте методи захисту від клептоатак наразі зводяться до традиційного криптоаналізу потенційно вразливих систем та видачі певних інтуїтивних рекомендацій щодо процесу розробки програмно-апаратних комплексів.*

Виділення недосліджених частин загальної проблеми. *Межі інтересів клептографії мають бути значно ширші ніж дослідження закладок у криптосистемах та охоплювати теорію і практику створення та виявлення таємних каналів витоку конфіденційних даних принаймі в системах захисту інформаційних систем.*

Постановка завдання. *Метою статті є аналіз причин виникнення клептографії як науки та напрямки її розвитку в системі знань з інформаційної безпеки, зокрема її зв'язок з криптографією та стеганографією.*

Виклад основного матеріалу. *Досліджено причини виникнення клептографії як науки та її місце в системі знань з інформаційної безпеки. Надані загальні рекомендації щодо захисту систем від клептографічних атак.*

Висновки. *Автори вважають, що до сфери клептографії слід віднести не тільки закладки у криптографічних системах, але й усі питання щодо методів і технологій створення та виявлення клептографічних каналів (штучно створених таємних каналів витоку конфіденційних даних) і виявлення клептоатак (обходу антивірусів, міжмережевих екранів та інших засобів інформаційної безпеки тощо) в інформаційних системах.*

Ключові слова: *клептографія, стеганографія, криптографія, клептографічний канал, реінжиніринг, інформаційна безпека.*

Рис.:2. Табл.1. Бібл.13.

Актуальність теми дослідження. Тайнопис, яким займаються криптографія чи стеганографія, з давніх часів був переважно прерогативою держави та військових (у середні віки – ще й церкви). Усі розробки технологій захисту інформації та відповідні наукові дослідження проводились у надрах спецслужб за завісою таємничості. Однак розвиток технологій та потреби суспільства у захисті зростаючих об'ємів інформації, що передаються або зберігаються, спонукало повільне перетікання накоплених спецслужбами знань і технологій у відкрите середовище із розгортанням подальших досліджень в різних наукових центрах.

Так, початком становлення *криптографії* як науки можна рахувати 1949 рік, коли була опублікована розсекречена робота Клода Шеннона «Теорія зв'язку в таємних системах» [1]. Під час Другої світової війни Шеннон займався зломом ворожих шифрів і саме він почав першим вивчати криптографію, використовуючи системний підхід. Наприклад, він дав визначення «цілком стійкого шифру» (шифру, який не можна зламати, маючи лише зашифроване повідомлення) та довів, що такі шифри можуть існувати (шифр Вернама).

На сьогоднішній день, з розвитком сучасних технологій, переважна більшість людей у повсякденному житті так чи інакше користується так званою "*цивільною криптографією*" – тобто криптографією, яка, на відміну від державної чи військової криптографії, покликана задовольняти потреби приватних осіб та організацій. Цивільна криптографія присутня у мобільному зв'язку, у банківських картах, в інтернет-браузерах при передачі інформації протоколом SSL/TLS тощо. З'явились навіть побутові прилади, які підключені до Інтернету (технологія IoT, Internet-of-Things), – і звичайно ж, комунікації таких пристроїв між собою та їх власником мають бути захищені. Навіть автомобілі стали частиною IoT (концепція Connected Car) – а це питання безпеки не тільки особистої інформації водія, але і його життя.

За такою ж схемою у 90-х роках минулого сторіччя у відкритому просторі почала формуватися наука *стеганографія*. Незважаючи на те, що стеганографія як спосіб приховування секретних даних відома вже протягом тисячоліть, роком становлення сучасної стеганографії як науки можна вважати 1996 рік, коли на міжнародному семінарі InfoHiding-96 була введена єдина термінологія [2]. Методи "*цивільної стеганографії*" також зайняли своє місце у повсякденному житті суспільства, наприклад у таких технологіях, як цифрові водяні знаки (digital watermark) – для захисту авторських прав на цифровий об'єкт або цифрові відбитки пальців (digital fingerprinting) – для захисту виключного права на цифровий об'єкт.

Водночас користувачами цивільної криптографії або стеганографії стають не лише законослухняні громадяни, а й злочинці, шахраї чи терористи, які використовують сучасні технології для підготовки, скоєння та приховування злочинів. З погляду правоохоронних органів, криптографія (стеганографія) в їхніх руках безумовно дуже зручна та небезпечна зброя.

У зв'язку зі зростанням терористичних загроз суспільство вимагає вжити заходів, у тому числі найжорсткіших. Держава, як правило, із задоволенням йде назустріч таким побажанням і антитерористичні заходи, які проводять з боку держави, стали стосуватися також криптографії та стеганографії. Тому посилення вторгнення держави у цивільну криптографію – цілком очікувана та неминуча реакція державних інституцій і, насамперед, законодавців та спецслужб.

Постановка проблеми. З широким впровадженням сучасних інформаційних технологій у повсякденне життя все більше офіційних осіб стали заявляти, що для боротьби з тероризмом необхідно прийняти рішення на офіційному державному рівні про впровадження відповідних лазівок в інформаційні системи, мережі та засоби захисту, у тому числі у криптоалгоритми, які є державними стандартами. Не впадаючи в пафос слів про свободи та права людини, варто усвідомити, що ми стоїмо перед непростим вибором – гарантоване обмеження свобод чи можлива загроза десяткам, сотням, а то й тисячам життів. На жаль, однозначного рішення немає. Лазівки, призначені для захисту від тероризму, можуть стати зброєю для терористів у разі витоку конфіденційних даних про них (наприклад, лазівка в Connected Car дозволяє дистанційно керувати автомобілем). А чи

існують надійні способи забезпечення ексклюзивного доступу спецслужб до інформації користувача при збереженні достатнього рівня стійкості до сторонніх зловмисників? Цим питанням опікується наука *клептографія.*

Аналіз останніх досліджень і публікацій. Сучасні дослідження з клептографії, окрім класичних робіт [3-4], де впроваджено базові поняття та терміни, в основному присвячено виключно синтезу криптосистем із закладкам (огляд таких методів є в [5-6]). Проте методи захисту від клептоатак наразі зводяться до традиційного криптоаналізу потенційно вразливих систем та видачі певних інтуїтивних рекомендацій щодо процесу розробки програмно-апаратних комплексів. Більш того, на наш погляд, предмет досліджень клептографії має бути значно ширшим та охоплювати усі методи і технології створення та виявлення штучних каналів витоків чуттєвих даних з інформаційних систем та їх систем захисту.

Мета статті. Метою є аналіз причин виникнення клептографії як науки та напрямки її розвитку в системі знань з інформаційної безпеки, зокрема її зв'язок з криптографією та стеганографією.

Виклад основного матеріалу. Будь-яка держава намагається контролювати принаймні свій сегмент кіберпростору. Це можливо різними способами. Наприклад, за рахунок колаборації державних структур (насамперед спецслужб США, Китаю та Росії) з великими фірмами-виробниками мікроелектроніки, обчислювальної та телекомунікаційної техніки з метою створення можливості збирання інформації про користувачів та доступу до їх інформації. До публікацій Едварда Сноудена і оприлюднення конкретних прикладів ніхто не був упевнений, що це відбувається насправді.

На даний час у ЗМІ неодноразово з'являлися дані про співпрацю зі спецслужбами відомих виробників засобів телекомунікацій (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Однокласники), антивірусних систем (Касперский, Radware, McAfee), постачальників послуг електронної пошти та мережевих Інтернет-гігантів (Google, Yahoo, AT&T, CenturyLink, Verizon). Така співпраця включає розробку та вбудовування необхідних «бекдорів» з подальшою передачею спецслужбам таємних відомостей про вразливості в апаратному та програмному забезпеченні, в тому числі і про ключі шифрування, що діють.

Але така співпраця зі спецслужбами інколи може зіграти згубну роль для виробника. Яркою ілюстрацією цієї тези може служити 70-річна історія відомої швейцарської компанії Crypto AG, яка була заснована Б. Хагеліном у 1952 році та спеціалізувалася на комунікаційній та інформаційній безпеці.

Шифрувальну машину М-209 розміром із мильницю Борис Хагелін розробив ще перед Другою світовою війною. Через свої габарити вона була цілком придатна для використання у польових умовах, тому США закупили ліцензією та виробили більше 140 000 таких шифраторів. Першу шифрувальну машинку, яку Б. Хагелін виробив після закінчення війни у Швейцарії, просто шокувала американців - вона була занадто надійна. Тому за їх наполегливою вимогою компанія Crypto AG стала випускати шифратори з керованою стійкістю. Фактично це стало початком операції «Рубікон», однією з найбільших розвідувальних операцій з часів Другої світової війни [7].

У 1970 році компанія Crypto AG була викуплена через посередників у спільну власність ЦРУ США та БНД (федеральної служби розвідки) Німеччини. З того часу спецслужби (США, Німеччини та Великобританії) могли давати розробникам прямі вказівки

та читати секретні телеграми як можливих супротивників, так і дружніх країн. Шифратори Crypto AG купувалась багатьма країнами світу для організації зв'язку у військових відомствах та зі своїми дипломатичними представництвами. При цьому випускалися два типи машин: з якісними криптографічними алгоритмами (їх отримували Швейцарія, Швеція та деякі країни НАТО) та варіанти машин з вбудованим «бекдором», які дуже легко зламувалися тими, хто знав, як це можна зробити. Таку техніку отримували інші держави. Усього дешифрувалися секретні шифртелеграми понад ста країн, включаючи Іспанію, Італію, Ватикан, Пакистан, Аргентину, Іран, Лівію та інші арабські країни. Тому ЦРУ і БНД мали у своєму розпорядженні, наприклад, всю повноту інформації про Фолклендську війну 1982 року, про теракт у берлінській дискотеці «Ла Бель» у 1986 році або про захоплення заручників в Ірані в 1979 році — і все завдяки невеликій швейцарській компанії в кантоні Цуг.

В останніх лінійках шифраторів Grypto AG (Cryptomatic, Cryptofax, Cryptovox тощо) були реалізовані складні криптоалгоритми та нові криптографічні конструкції, які враховували зростання обчислювальних потужностей у світі. Усі вони були електронними пристроями, реалізованими на сучасній елементній базі, багатошарових друкованих платах із захищеними спеціалізованими процесорами для виконання криптографічних перетворень й захищеною пам'яттю, де зберігалися специфічні криптографічні параметри. У цих засобах була реалізована багатоступенева система ключів:

- структурні ключі, які були згенеровані виробником для кожного конкретного клієнта (відомства, країни);
- змінні довгострокові ключі, що змінювалися з певною періодичністю;
- сеансові ключі для кожного конкретного повідомлення.

При чому, структурні ключі були відомі виробнику, довгострокові ключі генерувалися по відомому виробнику алгоритму і мали деякі особливості. Крім того, структура самого шифрованого повідомлення включала також низку синхронізуючих елементів, що були отримані шляхом певних математичних перетворень над елементами ключів, криптографічними параметрами, мітками часу тощо. У разі потокового шифрування, синхропакети для початкової і автоматичної повторної синхронізації також формувалися специфічним чином. Кожен такий елемент ніс в собі певні відомості, які дозволяли будувати додаткові рівняння відносно елементів ключів і параметрів криптоперетвореня, що загалом суттєво полегшувало задачу криптоаналітику.

У 2018 році після ряду скандалів Crypto AG була ліквідована, а Федеральна прокуратура Швейцарії, яка проводила розслідування діяльності компанії, зробила висновок, що операція «Рубікон», що проводилася у рамках співпраці «дружніх спецслужб», була цілком легальною і не суперечила як тодішнім, так і нинішнім правовим засадам та положенням.

Цей приклад показує, що спецслужби завжди приділяли увагу забезпеченню контролю чуттєвих технологій, що з'являлися на ринку. В їх надрах накоплено відповідний науково обґрунтований досвід для вирішення таких проблем. І це стосується на тільки криптографії, а й телекомунікаційних технологій та програмного забезпечення (у першу чергу операційних та антивірусних систем).

З широким впровадження сучасних інформаційних технологій в повсякдення життя все більше і більше офіційних осіб стали заявляти про необхідність ухвалення на офіційному державному рівні рішення про впровадження вразливостей в інформаційні системи, мережі

та пристрої, а також про обов'язкове впровадження лазівок у криптоалгоритми, які є державними стандартами. На даний час відомо як мінімум про два алгоритми, які були затверджені в США як федеральні стандарти і мають відповідні «бекдори».

Перший випадок - це стандарт криптографії з депонуванням ключів (проект Skipjack), де бекдор передбачався на апаратному рівні [8]. На початку дев'яностих минулого століття уряд США ініціював масовий випуск мікросхеми Clipper chip (VLSO MYK-78). Передбачалося, що вона встановлюватиметься у всі телефони і шифруватиме голосовий зв'язок, залишаючи АНБ можливість простого розшифровування за рахунок вбудованого бекдору. У центрі концепції Clipper була система депонування ключів (key escrow). На кожному пристрої з шифрувальним чіпом встановлювався криптоключ, який передавався уряду для депонування. Депонований ключ складався з двох частин, що окремо зберігалися в уповноважених урядових відомствах. Мікросхема генерувала сеансовий ключ, за допомогою якого шифрувала відкрите текстове повідомлення. Отриманий ключ шифрувався за допомогою ключа, що депонується. Після цього в зашифрованому вигляді, разом з ідентифікаційним номером мікросхеми, він приєднувався до шифрованого тексту. Якщо потрібно було побачити вміст повідомлення, зашифрованого з Clipper Chip, правоохоронці запитували депонований ключ у відповідних відомств. І вже використовуючи його, розшифровували сеансовий ключ і читали відкритий текст повідомлення. Тільки виняткова дорожнеча проекту Skipjack не дозволила перетворити його на життя.

Другий випадок – це криптографічний генератор псевдовипадкових чисел NIST SP 800-90A, який використовує криптографію з еліптичною кривою (Dual_EC_DRBG, Dual Elliptic Curve Deterministic Random Bit Generator) [9]. Вважається, що АНБ США зберігає закритий ключ, який разом з помилками зміщення Dual_EC_DRBG дозволяє розшифровувати трафік SSL між комп'ютерами. Більш того, цей стандарт був успішно просунутий у міжнародні стандарти [10].

На даний час розгортається скандал щодо створення стандартів постквантової криптографії (PQC). Деніел Бернштейн, експерт з університету Чикаго, вважає [11], що NIST при участі АНБ припустився навмисних або випадкових помилок у розрахунках безпеки нових стандартів типу Kyber512. Цілком ймовірно, що бекдори закладено при розробці інших стандартів шифрування і не тільки у США.

Фахівці з криптоаналізу жартують, що на ринку завжди присутні лише два типи криптографічних продуктів: з відомими лазівками та ще не виявленими. Причому непомітними ці бекдори можуть залишатися роками. Постає питання: а чи взагалі існують надійні методи забезпечення ексклюзивного доступу спецслужб до інформації користувача при збереженні достатнього рівня стійкості від стороннього порушника?

І тут на вирішення цього питання з надр спецслужб у повсякденне життя виринає та формується ще одна наука - ***клептографія*** (англ. keptography), яка вивчає теорію і практику побудови інформаційних систем, що містять безпечні та приховані штучні канали витоку секретної інформації шляхом впровадження вразливостей у систему захисту інформації.

Термін клептографія з'явився у 1998 році завдяки роботі відомих фахівців з криптографії А. Янга та М. Юнга [3-4]. Спочатку вони називали клептографією впровадження бекдора, що важко виявляється, виключно в схемах асиметричної криптографії. Такий бекдор давав можливість обчислити секретний ключ користувача за його відкритим ключем, але тільки тим, хто знав секрет. Згодом, вони розширили межі клептографії на інші види криптоалгоритмів, включаючи криптографічні протоколи.

Клептографія, як напрямок інформаційної безпеки, тісно пов'язана з криптографією та стегенографією (рис.1).

Зв'язок клептографії з криптографією обумовлено тим, що об'єктом її досліджень є клептографічна закладка, яка є частиною криптосистеми. Методи криптоаналізу часто використовуються для виявлення клептозакладок, тобто одночасно є інструментами клептоаналізу.

Клептографія близька також до стеганографії: їх базовим елементом є прихований канал (анг. subliminal channel, підсвідомий канал), який вперше запропонував Симмонс [12]. Будь-яка клептографічна атака ґрунтується на прихованому каналі передачі інформації. Саме вони у поєднанні з додатковими криптографічними методами забезпечують не виявлення цих атак.

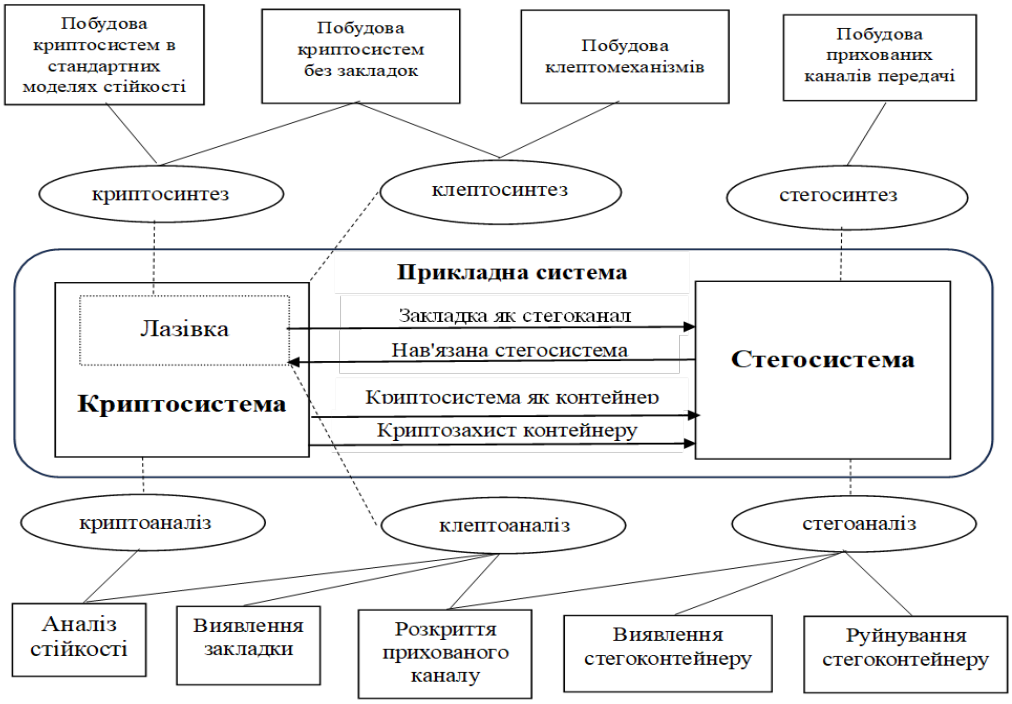

Рис.1. Зв'язок клептографії з криптографією та стеганографією

Клептографічні методи дозволяють довести до досконалості приховування факту передачі додаткової інформації. У цьому сенсі простежується подібність до стеганографії, але є і відмінності (табл.1). Приховані клептографічні канали є частиною криптоалгоритму і дозволяють непомітно передавати інформацію з криптографічної системи або, навпаки, до криптографічної системи. Наприклад, додаткова інформація може міститись у цифровому підписі або у відкритому ключі шифрування.

Терміни клептографії лише формуються, наведемо деякі з них:

- клептографічний механізм (закладка, клептографічна лазівка) - особливість дизайну системи захисту, що дозволяє розробнику, який впровадив даний механізм, створювати канал витоку секретних даних;
- клептографічна атака – можливі зловмисні сценарії, що можуть виконуватися розробником закладки: клептографічна модифікація системи захисту, побудова системи захисту з закладкою, використання можливостей закладок тощо;

- стійкість до клептографічних атак – властивість системи, що полягає у неможливості побудови непомітної закладки або каналу витоку.

- клептографічний канал витоку – канал непомітного витоку секрету (прихований канал, subliminal channel), який практично може отримати розробник закладки і не можуть отримати інші учасники системи.

Таблиця 1. Відмінність методів клептографії та стеганографії

Критерій порівняння	Клептографія	Стеганографія
Мета	Корекція роботи системи в інтересах розробника чи спецслужби	Приховування факту передачі інформації між користувачами
Рівень абстракції	На рівні крипто протоколу	На рівні передачі даних (залежить від типу даних та параметрів мережі)
Спосіб застосування	Таємна модифікація системи або впровадження лазівки на етапі розробки	Попереднє узгодження між користувачами стегосистеми
Спосіб впровадження	Інтегрується реалізацію системи	Сторонній модуль, програма, плагін
Щільність передачі	Відносно висока	Відносно низька
Вектор протидії	Збереження захисних властивостей системи користувача	Унеможливлення обміну прихованою інформацією
Протидія передачі	Стійкий клептомеханізм не може бути виявленим чи отфільтрований без порушення роботи системи	Псування контейнеру без порушення загальної роботи системи

Надійний клептографічний канал передачі даних повинен володіти наступними властивостями:

- *невиявленістю* - що означає неможливість виявлення клептографічної атаки виключно за зовнішніми ознаками, якщо система захисту (криптосистема в узькому сексі) є «чорною скринькою»;
- *стійкості до злому без проведення реінжинірингу* – неможливість перехоплення інформації без знання внутрішнього устрою системи захисту, тобто у рамках моделі «чорної скриньки»;
- *стійкості до злому групи пристроїв у результаті успішного реінжинірингу одного з них* - якщо група пристроїв працює за однаковим алгоритмом і з тими самими даними, то визначення в результаті реінжинірингу внутрішньої структури і стану одного з пристроїв не дозволяє визначити стан інших пристроїв групи, отже, і їх вихідні значення;
- *непередбачуваності вліво* - говорять, що послідовність непередбачувана вліво, якщо за довільною кількістю елементів послідовності неможливо визначити її попередні елементи. Тобто йдеться про непередбачуваність вліво для внутрішнього стану криптосистеми. Це актуально, наприклад, для недеструктивного зворотного проектування. Атака називається стійкою до цього виду аналізу, якщо навіть при повному знанні внутрішньої схеми пристрою та її поточного стану неможливо дізнатися про її попередній стан;
- *повної непередбачуваності* - мається на увазі непередбачуваність вліво, а також неможливість визначення наступних станів системи захисту (непередбачуваність вправо). Очевидно, що якщо нападнику вдається визначити внутрішній стан системи і значення усіх змінних, то для повної непередбачуваності системи потрібна наявність у ній джерела ентропії.

Зауважимо, деякі властивості є залежними, наприклад: друга властивість може виконуватися лише у тому випадку, якщо виконується перша. Третя властивість має сенс,

лише якщо виконується друга, а п'ята – лише якщо виконується четверта. Інші властивості незалежні.

Для відповіді на питання чи існує клептографічний канал та аналізу його властивостей необхідно, як правило, провести реінжиніринг (англ. reverse engineering) - процес дослідження деякого готового пристрою, програми, системи, а також документації з метою визначення внутрішнього устрою апарата чи програми для відтворення принципу роботи. Існують дві моделі реінжинірингу:

- *недеструктивний реінжиніринг*, який дозволяє використовувати пристрій після проведення процедури реінжинірингу. Така модель найчастіше застосовується до програмних систем та, інколи, до апаратних систем, якщо атакуюча сторона володіє відповідними неруйнівними технологіями;
- *деструктивний реінжиніринг*, який дозволяє визначити внутрішню схему системи, але проте подальше функціонування даного екземпляру системи стає неможливим. Реінжиніринг може виявити встановлену закладку і навіть інколи використовувати її.

При аналізі роботи клептографічних систем зазвичай виділяють наступних трьох учасників:

- *розробник* – володіє інформацією про лазівку $\boldsymbol{I_l}$, володіє секретним ключем до лазівки $\boldsymbol{K_l}$, але не володіє секретним ключем користувача $\boldsymbol{K_k}$;
- *користувач* – володіє секретним ключем користувача $\boldsymbol{K_k}$, у разі успішного реверс інжинірингу має інформацію про лазівку, але не володіє її секретним ключем $\boldsymbol{K_l}$;
- *зловмисник* – у разі успішного реверс-інжинірингу володіє інформацією про лазівку $\boldsymbol{I_l}$, але не володіє її секретним ключем $\boldsymbol{K_l}$, а також секретним ключем користувача $\boldsymbol{K_k}$.

Передбачається, що зловмисник успішно провів реверс-інжиніринг до одного або кількох подібних пристроїв та отримав інформацію про лазівку $\boldsymbol{I_l}$: код і вміст енергонезалежної пам'яті. Передбачається також, що зловмисник має доступ до всієї публічної інформації, включаючи загальнодоступні алгоритми, відкриті ключі, зашифровані тексти, підписи тощо. При цьому можна виділити два типи зловмисника:

- *зловмисник-відрізняльник* – мета якого полягає в тому, щоб відрізнити чесну реалізацію від нечесної;
- *зловмисник-криптоаналітик* – його мета полягає в тому, щоб зламати безпеку даного пристрою, який ніколи не піддавався реверс-інженірингу (це може включати знаходження закритого ключа користувача, дешифрування інформації, зашифрованих з відкритим ключем, підробку підпису тощо).

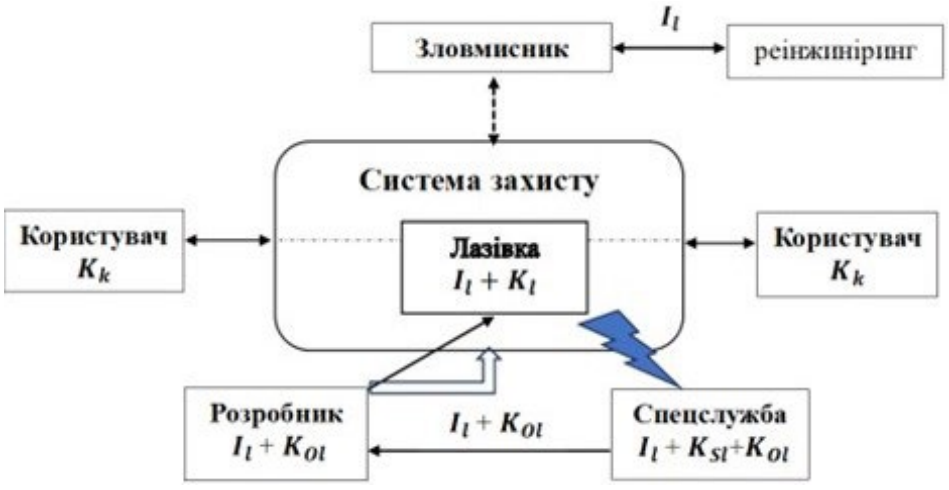

Рис.2. Механізм взаємодії учасників клептографічної системи

Зважаючи на тенденції останніх років, рольову модель можна видозмінити, додавши ще одного учасника – *спецслужбу* – та обмежити рівень знання розробника (рис.2). У цій новій моделі разом із «користувачем» та «зловмисником» діють:

- *спецслужба* - має інформацію про лазівку $\boldsymbol{I_l}$, володіє секретним ключем до лазівки $\boldsymbol{K_{Sl}}$, не володіє секретним ключем користувача $\boldsymbol{K_k}$;
- *розробник* - має інформацію про лазівку $\boldsymbol{I_l}$, володіє відкритим ключем лазівки $\boldsymbol{K_{Ol}}$, не володіє секретним ключем до лазівки $\boldsymbol{K_{Sl}}$, не володіє секретним ключем користувача $\boldsymbol{K_k}$.

Спецслужба видає розробнику інструкції з реалізації лазівки та відкритий ключ $\boldsymbol{K_{Ol}}$, за допомогою якого шифруватимуться дані, що видаються через лазівку. Розробник знає весь механізм роботи $\boldsymbol{I_l}$, але не знає секретного ключа $\boldsymbol{K_{Sl}}$, тому при використанні не зможе отримати доступ до даних користувача (тобто користувач захищений не тільки від стороннього порушника, але і від розробника).

Зловмисник до проведення реверс-інжинірингу має менші можливості, ніж розробник, а після його проведення він може отримати механізм роботи лазівки $\boldsymbol{I_l}$. Крім того, у зловмисника, якщо у нього є відповідні спроможності, є можливість вивчити архітектуру побудови системи захисту, розробити та впровадити свою закладку для створення клептографічного каналу.

На даний час існує тільки загальні рекомендації щодо захисту від клептографічних атак в криптосистемах, такі як проведення комплексного аналізу структури криптосистеми із залученням фахівців у галузі криптографії або композиція (каскадування) криптоперетворень, що мають походження з різних джерел:

1. Перед використанням криптографічного примітиву, його структура має бути ретельно вивчена та оцінена. Не можна беззастережно довіряти апаратним компонентам із заданою специфікацією (необхідна перевірка реалізації на відповідність специфікації, а також вивчення самої специфікації). Навіть програмні реалізації можуть бути небезпечні, особливо якщо вихідний код і документація розробника недоступні для перевірки.
2. Проходження тестів за формальними критеріями не гарантує відсутності прихованих лазівок. Зокрема, не можна приймати рішення про довіру лише виходячи з великого статистичного дослідження. Очевидно, для будь-якого фіксованого набору критеріїв можна побудувати криптосистему з лазівкою, яка задовольнятиме цим критеріям.
3. Непоганий захист від наявності прихованих лазівок у криптоалгоритмах дає композиція (каскадування) криптоперетворень, що мають походження з різних джерел.
4. Важливим є контроль за випадковістю. Цілком необхідно, щоб алгоритми генерації випадкових величин, що використовуються в криптографічних примітивах, були відкриті для користувача. Якщо є програмне забезпечення для вироблення ключів – воно має бути абсолютно надійним та довіреним. Добре щоб була можливість використовувати стороннє джерело випадкових чисел.
5. Краще якщо джерело випадковості, генератор ключів та алгоритм, що їх використовує – були три роздільні компоненти. При цьому має бути виключена можливість їхнього обходу, самі вони – з надійного джерела, а канали, що їх пов'язують, не допускають витоку інформації.

Поки що можна констатувати, що ліцензування систем захисту є єдиним способом боротьби з клептографією (якщо не враховувати інтереси спецслужб).

Загалом, можна виділити подальші напрямки клептографічних досліджень:

- побудова клептографічного каналу витоку шляхом модифікації стандартної системи захисту;
- створення нових систем захисту з вбудованим клептографічним каналом;

- виявлення клептографічних закладок як у загальній схемі системи захисту, так і у її конкретній реалізації;
- побудова системи захисту з гарантованою відсутністю клептографічного каналу витоку;
- побудова системи захисту із мінімізацією можливостей вбудовування клептозакладки.

У ході дослідження за даними напрямками виникає ще ряд пов'язаних проблем:

- відсутність достатньої формалізації клептографії (не зважаючи на те, що наразі вже відомі чисельні практичні та теоретичні клептографічні системи, досі не сформована більш-менш загальна теорія);
- неадекватність наявних моделей надійності систем захисту у контексті клептографічних задач;
- відсутність методів оцінки ризиків, пов'язаних з клептографічними атаками;
- відсутність методів побудови елементів захисту з доведеною відсутністю клептозакладок;
- відсутність критеріїв оцінки потенційних клептографічних можливостей систем захисту та інші.

Висновки. В інформаційній безпеці все винаходять щонайменше двічі: один раз спецслужбами "у закриту", а вдруге - науковцями "у відкриту" (в деяких випадках навіть більше, ніж двічі - і це нормально). Криптографія цей шлях вже пройшла, стеганографія ще проходить, а для клептографії усе тільки починається.

Усталений підхід до клептографії, що вивчає тільки методи потайного ослаблення елементів систем шифрування (генерації ключів, цифрового підпису, обміну ключами, генераторів псевдовипадкових чисел, криптоалгоритмів) для їх використання з нелегальною метою, є підходом *в узькому сенсі*, який відносить клептографію до розділу криптографії.

Але створення та виявлення клептографічних каналів актуально і для інших систем захисту інформації. Тому автори роботи стверджують, що межі клептографії повинні бути значно ширшими і не обмежуються тільки криптосистемами. Нашим даним загрожують не тільки шпигуни та хакери, а й виробники широкого діапазону пристроїв захисту, каналів зв'язку та інформаційних систем, а, подекуди, до них додаються ще "неконтрольовані" спецслужби.

У зв'язку з цим, наука клептографія *в широкому сенсі* має досліджувати усі механізми непомітного викрадення інформації користувача з інформаційних систем. Наприклад, близько до класичних задач клептографії примикають програмні та апаратні закладки (у тому числі систем захисту інформації), які часто встановлюються самими розробниками або їх контрагентами. Тому вважаємо, що до сфери інтересів клептографії слід віднести усі питання щодо методів і технологій створення та виявлення клептографічних каналів (штучно створених таємних каналів витоку конфіденційних даних), а також виявлення клептографічних атак (обходу антивірусів, міжмережевих екранів та інших засобів інформаційної безпеки тощо).

Список використаних джерел

1. Shannon, C. E. Communication Theory of Secrecy Systems / C. E. Shannon // Bell System Technical Journal. – 1949. – Vol. 28. Is. 4, oct. – P. 656-715.

2. Phitzmann, B. Information hiding terminology / B. Phitzmann // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science. – 1996. – Vol. 1174. – P. 374-350.

3. Young A. Kleptography: using Cryptography against Cryptography / A. Young, M. Yung // EUROCRYPT'97. Series: Lecture Notes in Computer Science. – Springer, 1998. – Vol. 1233. – P. 62-74.

4. Young, A. Malicious Cryptography. Exposing Cryptovirology / A. Young, M. Yung. – Wiley Publishing, Inc. 2004. – 419 p.

5. Коваленко, Б. А. Методи та моделі побудови криптосистем стійких до клептографічних модифікацій : дис. ктн за спеціальністю 05.13.21. / Б. А. Коваленко; НАУ. – Київ, 2019.

6. Kovalenko B. Kleptography trapdoor free cryptographic protocols [Electronic resource] / B. Kovalenko, A. Kudin // Cryptology ePrint Archive, Report. – 2018. – 989. – Access mode https://eprint.iacr.org/2018/989.

7. Operation Rubikon ZDFmediathek. [Electronic resource]. – Access mode https://www.zdf.de/politik/frontal/operation-rubikon-100.html

8. National Institute of Standards and Technology. Escrowed Encryption Standard. NIST FIPS PUB 185. – U.S. Department of Commerce, 1994.

9. National Institute of Standards and Technology. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A, Rev. 1, 2012 [Electronic resource] First version June 2006, second version March 2007. – Access mode : http://csrc.nist.gov/publications/ PubsSPs.html#800-90A.

10. ISO/IEC 18031:2005. Information technology – Security techniques – Random bit generation.

11. Matthew Sparkes Mathematician warns US spies may be weakening next-gen encryption [Electronic resource] // NewScientist. – 2023. – 10 October. – Access mode : https://www.newscientist.com/article/2396510-mathematician-warns-us-spies-may-be-weakening-next-gen-encryption

12. Simmons, G. The Prisoners' Problem and the Subliminal Channel / G. Simmons // Plenum Press. In Proceedings of Crypto '83. – 1984. – P. 51-67.

References

1. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal, 28*, 4, 656-715.

2. Phitzmann, B. (1996). Information hiding terminology. *Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174,* 374-350.

3. Young, A., Yung, M. (1998). Kleptography: using Cryptography against Cryptography. *In book: EURO-CRYPT'97 (series: Lecture Notes in Computer Science), 1233,* 62–74.

4. Young, A., Yung, M. (2004). Malicious Cryptography. Exposing Cryptovirology. Wiley Publishing, Inc.

5. Kovalenko, B. (2019). Methods and models for developing cryptosystems resistant to kleptographic modifications : *Candidate's thesis*. Kyiv, National Aviation University.

6. Kovalenko, B., Kudin, A. (2018). Kleptography trapdoor free cryptographic protocols. *Cryptology ePrint Archive, Report 2018/989.* https://eprint.iacr.org/2018/989.

7. Operation Rubikon. ZDFmediathek. (February 11, 2020). https://www.zdf.de/politik/frontal/operation-rubikon-100.html

8. National Institute of Standards and Technology. (1994). Escrowed Encryption Standard. NIST FIPS PUB 185, U.S. Department of Commerce.

9. National Institute of Standards and Technology. (2007). Recommendation for Random Number Generation Using Deterministic Random Bit Generators. – NIST Special Publication 800-90A, Rev. 1, 2012. First version June 2006, second ver-sion March 2007. http://csrc.nist.gov/publications/ PubsSPs.html#800-90A.

10. ISO/IEC 18031:2005. Information technology – Security techniques – Random bit generation.

11. Sparkes, M. (October 10, 2023). Mathematician warns US spies may be weakening next-gen encryption. *NewScientist.* https://www.newscientist.com/ article/2396510-mathematician-warns-us-spies-may-be-weakening-next-gen-encryption

12. Simmons, G. (1984). The Prisoners' Problem and the Subliminal Channel. Plenum Press. *In Proceedings of Crypto '83,* 51-67.

Отримано 15.09.2023

UDC 004.056

Yuliia Tkach[1], Mykhailo Shelest[2], Maryna Synenko[3], Taras Petrenko[4]

[1] Doctor of Pedagogical Sciences, Head of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University
E-mail: tkachym79@gmail.com **ORCHID:** https://orcid.org/0000-0002-8565-0525 **Scopus Author ID:** 57193026076

[2] Doctor of Technical Sciences, Professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University
E-mail: mishel3141@gmail.com **ORCHID:** https://orcid.org/0000-0003-1090-0371 **Scopus Author ID:** 57211429755

[3] PhD in Physics and Mathematics, Associate Professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University
E-mail: mara.a.snnk@gmail.com **ORCHID:** https://orcid.org/0000-0002-8961-533X **Scopus Author ID:** 55884350800

[4] PhD in Technical Science, Associate Professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University
E-mail: 4650364@gmail.com **ORCHID:** https://orcid.org/0000-0001-5571-3815 **Scopus Author ID:** 57193026484

THE HISTORY OF KLEPTOGRAPHY AND ITS PLACE IN INFORMATION SECURITY

Urgency of the research. *Intensive informatization of society creates new threats: users of modern IT technologies become not only law-abiding citizens, but also criminals, fraudsters or terrorists who use them to commit crimes. Therefore, any state tries to control, at least, its segment of cyberspace. Solving such a problem may require methods studied by a new scientific discipline - kleptography.*

Target setting. *In order to fight terrorism, it is necessary to make a decision at the official state level to implement appropriate control of information systems and networks. And are there reliable ways to ensure exclusive access of special services to user information while maintaining a sufficient level of resistance to third-party attackers? These questions are solved by kleptography.*

Actual scientific researches and issues analysis. *Modern research on kleptography, apart from the classic works of A. Young and M. Jung, where the basic concepts and terms are introduced, is mainly devoted exclusively to the synthesis of cryptosystems with backdoors. However, methods of protection against kleptoattacks are currently limited to traditional cryptanalysis of potentially vulnerable systems and issuing certain intuitive recommendations regarding the process of developing software and hardware complexes.*

Uninvestigated parts of general matters defining. *The scope of interests of kleptography should be much wider than the research of backdoors in cryptosystems and include the theory and practice of creating and detecting secret channels of leakage of confidential data in information systems.*

The research objective. *The purpose of the article is to analyze the reasons for the emergence of kleptography as a science and the direction of its development in the information security knowledge system, in particular its connection with cryptography and steganography.*

The statement of basic materials*. The reasons for the emergence of kleptography as a science and its place in the system of information security knowledge have been studied. General recommendations for protecting systems against kleptographic attacks are provided.*

Conclusions. *The authors believe that the field of kleptography should include not only backdoors in cryptographic systems, but also all issues related to the methods and technologies of creating and detecting kleptographic channels (artificially created secret channels for leaking confidential data) and detecting kleptoattacks (bypassing antiviruses, internet screens and other means information security, etc.).*

Keywords: *kleptography, steganography, cryptography, kleptographic channel, reverse engineering, information security.*
Fig.:2. Table:1. References:15.

Ткач Ю., Шелест М., Синенко М., Петренко Т. Історія виникнення клептографії та її місце в безпеці інформації. *Технічні науки та технології.* 2023. № 3(33). С. 150-161.