DOI: 10.25140/2411-5363-2023-4(34)-91-103
УДК 004.056.53

Анатолій Борода[1], Тарас Петренко[2]

[1]кандидат технічних наук, головний науковий співробітник науково-дослідного відділу науково-дослідного центру
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (Київ, Україна)
E-mail: anv_boroda@ukr.net. **ORCID:** https://orcid.org/0009-0007-9302-8297. **ResearcherID:** JRX-2757-2023

[2]кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: mail_taras@stu.cn.ua. **ORCID**: https://orcid.org/0000-0001-5571-3815. **ResearcherID:** G-5801-2014

ВПЛИВ АТАК ЗА ПОБІЧНИМИ КАНАЛАМИ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Усім відомо, що для того, щоб криптографічна система забезпечувала безпеку інформації необхідно, щоб секретні ключі, які використовуються в криптографічних алгоритмах, залишалися секретними за будь-яких обставин. Проте на практиці реалізація та експлуатація криптографічних механізмів безпеки ніколи не забезпечує «ідеального» захисту інформації. Однією з вразливостей цих систем є незахищеність криптографічних модулів від з атак за побічними каналами, яка завжди буде серйозною загрозою безпеці криптографічних модулів та, як наслідок, інформаційній безпеці обчислювальних і комунікаційних систем. Тому під час реалізації криптографічних механізмів захисту повинні оцінюватися всі можливості таких атак і враховуватися всі аспекти їх застосування.

Метою статті є дослідження атак за побічними каналами на реалізації механізмів криптозахисту, аналіз особливостей їх реалізації та огляд механізмів забезпечення інформаційної безпеки під час деструктивних впливів цих атак. У роботі розглядається один із практичних напрямів криптоаналізу – атаки за побічними каналами на реалізації механізмів криптозахисту. Досліджуються відмінності між теоретичним криптоаналізом і атаками за побічними каналами. Аналізуються можливості атак за побічними каналами та особливості виконання атак з ін'єкції збоїв. Розглядаються особливості забезпечення інформаційної безпеки механізмів криптозахисту стосовно атак за побічними каналами. Доводиться необхідність врахування загрози цих атак при забезпеченні інформаційної безпеки обчислювальних і комунікаційних систем.

Ключові слова: *атаки за побічними каналами; криптосистема; інформаційна безпека.*
Рис.: 2. Бібл.: 19.

Актуальність теми дослідження. Важливим завданням при побудові обчислювальних і комунікаційних систем є забезпечення їх інформаційної безпеки. Будівельними блоками механізмів безпеки, заснованих на криптографії, є криптографічні примітиви[1], а саме криптографічні алгоритми – симетричні шифри, шифри з відкритим ключем та хеш-функції, які використовуються для реалізації необхідних функцій механізму безпеки. З погляду теоретичної криптографії не важливо, як ці примітиви будуть реалізовані – за допомогою програмного забезпечення, що виконується на звичайному комп'ютері, або в окремому спеціалізованому пристрої (криптографічному модулі, шифраторі), і т. ін. Тому в процесі теоретичного криптоаналізу криптосистем і протоколів безпеки спосіб реалізації не враховується. Але передбачається, що реалізація криптографічних примітивів задовольняє специфічним вимогам, а саме, що виконання криптографічних операцій (операцій з секретним ключем) відбувається всередині ідеального «чорного ящика», який забезпечує повну ізоляцію обчислювальних процесів, що в ньому відбуваються, від зовнішнього середовища. Тобто, неможливо отримати будь-яку інформацію про ці процеси, або зробити на них який-небудь вплив. Зважаючи на ці припущення, у теоретичній криптографії рівень безпеки оцінюється, з огляду на математичні властивості криптографічних алгоритмів і розмірів їхніх ключів.

Для того, щоб криптографічна система забезпечувала безпеку інформації необхідно, щоб секретні ключі, які використовуються в криптографічних алгоритмах реалізації безпеки, залишалися секретними (не були розкриті) при будь-яких обставинах. Самі криптографічні алгоритми, перш ніж вони будуть використовуватися в реальних криптосистемах, протягом довгого часу вивчаються великою кількістю

[1] Найнижчий рівень криптосистеми. Це найменші «цеглинки», або деталі, з яких вона може бути складена. Джерелом примітивів є математичні проблеми, що важко розв'язуються, (наприклад, проблема дискретного логарифма може служити основою односпрямованої функції) і спеціально створені конструкції (блокові шифри, хеш-функції).

експертів з метою виявлення вразливостей, і якщо такі вразливості не були виявлені – можуть вважатися досить надійними. Тому зловмисники швидше будуть намагатися атакувати ту частину криптосистеми, – так званий «криптографічний модуль», що реалізує криптографічні алгоритми.

Постановка проблеми. Навіть у повністю ізольованих від зовнішніх впливів системах, практичне застосування будь-яких криптографічних алгоритмів не забезпечує досконалий захист від несанкціонованого доступу як до зашифрованих даних, так і до інформації про суб'єктів обміну цими даними. Криптографічні алгоритми реалізуються програмно або апаратно деяким фізичним пристроєм, який у процесі роботи може взаємодіяти з іншими компонентами криптосистеми і з навколишнім середовищем, здійснюючи на них певний вплив, який може бути зафіксований ззовні. Ці взаємодії можуть контролюватися зловмисником і давати йому деяку інформацію, корисну для криптоаналізу. Така інформація називається побічною інформацією, а сам тип криптоаналітичних атак з використанням побічної інформації називається атаками за побічними каналами.

Такі атаки можуть використовуватися для несанкціонованого доступу до пам'яті криптографічного обладнання, де зберігається ключ-модифікатор алгоритму, який програмується виробником обладнання, є секретним і тільки йому відомим. За наявністю цього ключа (або алгоритму його генерації) у деяких випадках надалі можливе подолання криптозахисту інформаційних систем методами теоретичного криптоаналізу. З іншого боку, за допомогою атак за побічними каналами можливе відновлення невідомих фрагментів криптопротоколів та протоколів комунікаційного обладнання, знання яких надає можливість отримання доступу до інформації, що передається.

Саме тому атаки за побічними каналами є серйозною загрозою безпеці криптографічних модулів та, як наслідок, – інформаційній безпеці обчислювальних і комунікаційних систем. Тому при реалізації механізмів захисту повинні оцінюватися всі можливості таких атак і враховуватися всі аспекти їх застосування.

Аналіз останніх досліджень і публікацій. Перша інформація щодо застосування атаки за побічними каналами сходить до 1965 року [1]. У цьому році підрозділ британської розвідки MI5 намагався розкрити шифр єгипетського посольства в Лондоні, але ці зусилля не мали успіху через недостатність обчислювального ресурсу. Тоді було запропоновано таємно розмістити мікрофон поруч з ротором єгипетської електромеханічної шифромашини, щоб вловлювати звуки, які вона видавала. Прослуховуючи клацання роторів при скиданні їх шифрувальником щоранку в початкове положення, в MI5 успішно визначали початкові положення 2 або 3 роторів шифромашини. Ця додаткова інформація зменшувала обсяг обчислень, необхідних для розкриття шифру, внаслідок чого MI5 могла читати листування посольства протягом багатьох років.

Подібні атаки були відомі і застосовувалися ще в 1980-х роках, проте широке поширення атаки за побічними каналами отримали після публікації результатів криптоаналітика Пола Кохера в 1996 році [1]. Розроблений ним цілий клас атак базувався на тому, що є певна кореляція між результатами фізичних вимірювань деяких параметрів криптосистеми в різні моменти часу та процесом виконання в криптографічному модулі обчислень за участю секретних ключів. На отриманих Полом Кохером результатах ґрунтується багато піонерських ідей інших криптоаналітиків, які наукове співтовариство у сфері публічної криптографії відносить до атак за побічними каналами.

Відтоді атаками за побічними каналами називається клас криптоаналітичних атак, спрямований на використання тих чи інших вразливостей у практичній реалізації криптосистеми.

За способом використання побічних каналів атаки розділяються на дві категорії:
1) Пасивні: виконується лише аналіз поведінки цільового пристрою, наприклад:
- відстежується час виконання пристроєм (криптографічних) операцій;
- вимірюється споживання потужності;
- реєструється електромагнітне випромінювання.
Ця категорія має назву SCA-атак (Side Channel Analysis Attacks).
2) Активні: націлені на змінювання поведінки пристрою за допомогою:
- збоїв живлення та тактової синхронізації;
- потужних електромагнітних імпульсів;
- лазерних імпульсів різної частоти та інтенсивності.
Друга категорія зветься атаками з ін'єкції збоїв або FI (Fault Injection) атаками.

Сьогодні фахівцями з криптографічного захисту інформації досліджено багато типів атак побічними каналами та виокремлені загальні методи захисту від їх успішної реалізації.

Так, у 2008 р. було продемонстровано, як атаки типу DPA можна використовувати для відновлення ключів криптосистеми на RFID-картах. Зловмисники могли аналізувати енергоспоживання пристрою під час виконання операцій та використовувати цю інформацію для отримання секретних ключів [9]. Уже у 2013 р. дослідники провели експериментальну таймінг-атаку на Hash-based Message Authentication Code (HMAC), який використовується для перевірки цілісності повідомлень. Вони використовували варіації в часі виконання алгоритму HMAC для отримання секретного ключа. У 2018 р. були досліджені атаки на ECC-пам'ять апаратних криптосистем та виокремлені особливості захисту від них [17].

Проте, закономірно, із вдосконаленням атак постійно змінюються і заходи та механізми, призначені до їхньої протидії. Виробники вбудованих чипів і постачальники смарт-карток усвідомлюють загрози, які створює розробка і впровадження все більш досконалих атак за побічними каналами, і у відповідь реалізують комбінації контрзаходів, при цьому найбезпечніші смарткарти повинні містити поєднання апаратних і програмних функцій безпеки.

Звичайно, кожен контрзахід має свою ціну. Основні компроміси полягають у вартості виробництва апаратних систем захисту, їхньої продуктивності порівняно з програмними криптосистемами та їх стійкості до атак за побічними каналами. Ефективного захисту не можливо досягти на основі дешевих рішень. Тому сьогодні реально застосовні контрзаходи мають на меті зробити атаки за побічними каналами на криптографічні системи економічно не вигідними, але не можуть їм запобігти загалом.

Разом з тим, останні публікації в області аналізу побічних каналів свідчать про те, що найбільшої ефективності досягли активні атаки з ін'єкції збоїв. У деяких випадках ці атаки дозволяють відновлювати секретні ключі на основі мінімальної інформації про поведінку цільового пристрою: іноді достатньо взнавати, як пристрій спрацьовував у результаті ін'єкції збоїв – правильно чи ні.

Виділення недосліджених частин загальної проблеми. Нині у роботах вітчизняних та закордонних учених недостатньо уваги приділяється тим загрозам, що становлять для інформаційних та телекомунікаційних систем активні атаки за побічними каналами, які потребують розробки специфічних заходів протидії, і це не дозволяє повною мірою захиститися від існуючих атак цієї категорії, а також передбачати заходи щодо пом'якшення наслідків від подібних перспективних атак.

Мета статті. Ця стаття розглядає методи і прийоми, які використовуються в атаках за побічними каналами, дані щодо можливостей таких атак, стандартизовані підходи до тестування та оцінки механізмів безпеки. Обґрунтовується важливість розуміння методів та практичних можливостей атак за побічними каналами для забезпечення інформаційної безпеки в сучасних умовах.

Виклад основного матеріалу. Основна ідея атак за побічними каналами полягає в тому, щоб здійснювати спостереження за процесом обробки даних при виконанні криптографічного алгоритму й намагатися застосувати отриману таким чином побічну інформацію для послаблення стійкості механізмів безпеки.

1) **1. Відмінності між теоретичним криптоаналізом і атаками за побічними каналами [2].** Криптографічний примітив можна розглядати як мінімум із двох точок зору: з одного боку, його можна розглядати як абстрактний математичний об’єкт (перетворення, можливо параметризоване ключем, що перетворює деякі вхідні дані в деякі вихідні); з іншого боку, цей примітив реалізується належною програмою, яка виконується на певному процесорі, в конкретному обладнанні і, отже, буде мати конкретні характеристики. Перший погляд являє собою підхід з боку «класичного» криптоаналізу; а інший – з боку SCA-аналізу. Криптоаналіз за побічними каналами використовує конкретні характеристики реалізації криптографічного примітиву для відновлення секретних параметрів, які беруть участь у перетворенні. Методи SCA-аналізу є менш загальними, оскільки часто прив’язані до конкретної реалізації, але часто набагато більш потужними, ніж класичний криптоаналіз, і тому дуже серйозно розглядаються розробниками криптографічних пристроїв.

У багатьох випадках SCA-атаки можуть бути значно ефективніші, ніж криптоаналітичні атаки, які базуються на звичайних методах математичного аналізу, і такі SCA-атаки набагато практичніше здійснювати. Під час аналізу протоколу шифрувального пристрою або його програмного забезпечення, можна застосовувати певні формальні методи для моделювання роботи пристрою, щоб змоделювати вплив на нього ворожих дій противника й оцінити наскільки правильно, незважаючи на це, забезпечується функціонування пристрою. Таким чином можна отримати деяке уявлення про те, що в межах такої абстрактної моделі пристрій може протистояти ворожим атакам.

У традиційному криптоаналізі, при оцінці безпеки криптографічного протоколу переважно передбачається, що противник має повний опис протоколу, має у своєму розпорядженні всі відкриті ключі, і тільки не вистачає знання секретних ключів. Крім того, противник може перехопити деякі дані, що передаються між легальними учасниками шифрованого листування, і навіть може мати деякий контроль над природою цих даних (наприклад, шляхом вибору повідомлень в атаці на цифровий підпис методом селекції повідомлень, або шляхом вибору шифртексту в атаці на схему шифрування з відкритим ключем методом селекції шифртексту). Противник намагається розкрити криптопротокол або шляхом обернення того важкооборотного перетворення, що лежить у його основі, або використовуючи якусь ваду в побудові криптопротоколу.

У цьому випадку математична абстракція може бути дуже корисним інструментом у дослідженні криптографічних примітивів. Криптографи часто оцінюють безпеку шифрів, розглядаючи їх як математичні функції, які використовуються в ситуації, аналогічної наведеної на рис. 1.

Традиційно, надійні криптографічні алгоритми забезпечують безпеку проти супротивника, по відношенню до якого відповідне шифробладнання має властивості «чорного ящика», тобто забезпечує неможливість доступу до будь-якої інформації, пов'язаної з секретними даними учасників шифрованого листування. Однак такі моделі не завжди адекватні. Зокрема, безпека криптоалгоритму може бути зламана при можливості атак, які здійснюють крадіжку або підробку секретного ключа.

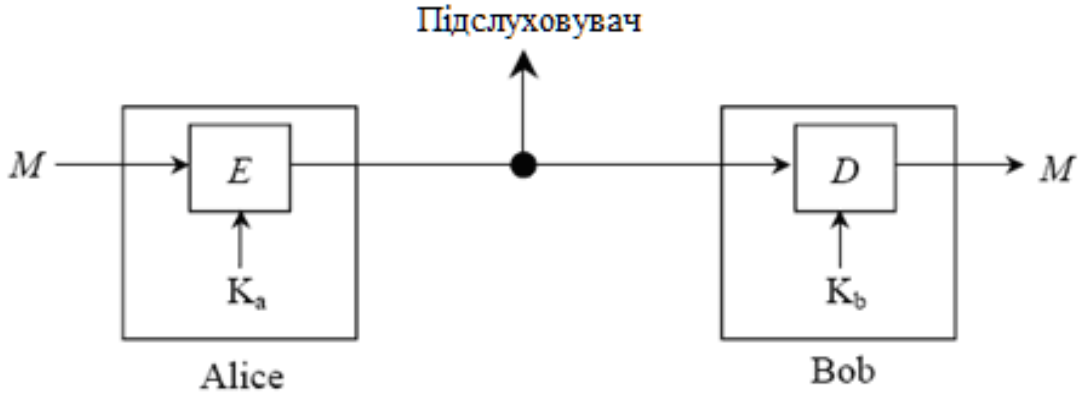

Рис. 1. Сценарій теоретичного криптоаналізу

Атаки, що розглядаються в цій традиційній криптографічній моделі, використовують математичні специфікації криптопротоколів.

Однак, якщо переходити від абстрактного поняття безпеки до її конкретного забезпечення в реальному фізичному світі, усе стає складніше. Безліч реальних нюансів, які абстрактна модель не враховує, стають значущими. Яка конструкція корпусу цього конкретного криптографічного пристрою? Які вихідні дані з пристрою противник може спостерігати, і якими вхідними даними противник може маніпулювати, щоб впливати на пристрій? У загальному випадку на ці питання важко відповісти, але при проєктуванні архітектури пристрою, що забезпечує захист від SCA-атак, обов'язковою є формулювання таких відповідей.

Крім того, часто фізичні процеси обчислень у процесі виконання криптоалгоритму можуть призводити до певних ефектів, які зможе спостерігати супротивник, і ці спостереження можуть іноді відображати чутливі внутрішні дані, які не повинні виходити за межі захищеного криптографічного модуля. Такий тип атак називають також аналізом за побічними каналами, так як у цьому випадку витоки інформації з модуля або пристрою відбуваються по інших каналах, на відміну від основних інтерфейсів призначених для обміну інформацією.

Здійснюючи фізичний напад на криптографічний пристрій, супротивник сподівається якимось чином підірвати його захисні властивості, зазвичай, витягуючи деякий секрет, який цей пристрій не повинен був розкривати. На перший погляд, природним шляхом досягнення цієї мети є прямий підхід: необхідно якимось чином обійти захист криптографічного пристрою і прочитати ці дані. Але такі атаки прямого типу можуть бути легко зірвані за допомогою застосування технологій захисту від несанкціонованого доступу (tamper-resistant) під час практичного проєктування криптографічного пристрою. Хоча цей прямий підхід часто може виявитися досить успішним, більш вірним є використання сімейства витончених непрямих підходів, у ході яких противник замість прямого втручання намагається викликати помилку у функціонуванні пристрою через деякі фізичні несправності, і якщо, не дивлячись на помилку, модуль продовжить працювати, він може в кінцевому підсумку розкрити досить інформації для відновлення супротивником секрету.

Останніми роками дослідники дедалі більше усвідомлюють можливість атак, що використовують специфічні властивості реалізації і конкретного обладнання (рис. 2).

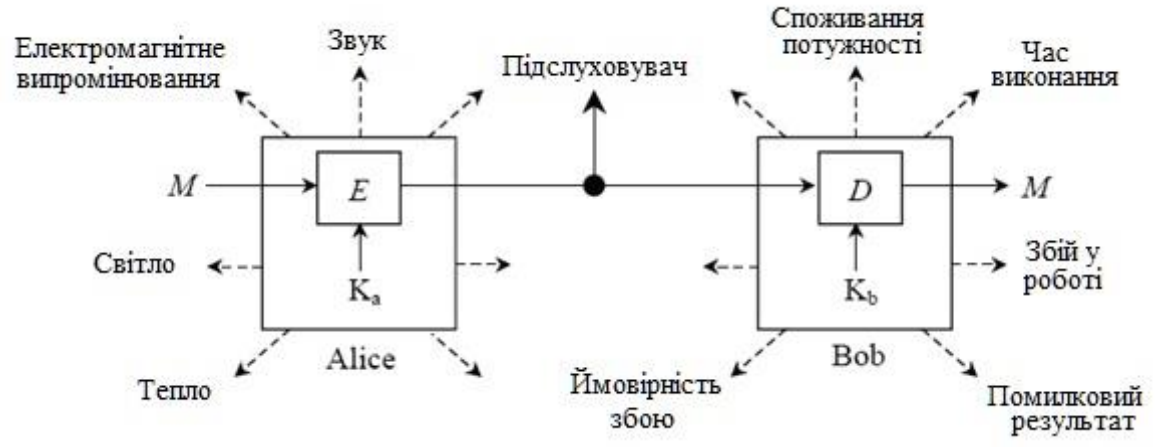

Рис. 2. Сценарій атаки, який включає використання побічних каналів

Такі SCA-атаки використовують деякий витік інформації в процесі виконання цього криптопротоколу і не враховуються в традиційних моделях безпеки. Наприклад, супротивник може бути в змозі контролювати споживану потужність або електромагнітне випромінювання, що генерується смарт-карткою під час виконання операцій з секретним ключем, таких як розшифрування і генерація підпису. Супротивник може також бути в змозі визначати час, що витрачається на виконання криптографічних операцій, або проаналізувати, як веде себе криптографічний пристрій при виникненні деяких збоїв. На практиці, побічна інформація може бути досить легко отримана, і тому важливо, щоб загроза SCA-атак була визначена кількісно при оцінці загальної безпеки системи в межах сценарію, представленого на рис. 2.

Відповідно до можливостей зловмисника в обох сценаріях, основні відмінності зазначених класів атак формулюються таким чином (табл. 1).

Таблиця 1 – Відмінності основних класів атак

Теоретичний криптоаналіз	SCA-атаки
Криптопримітиви розглядаються як абстрактні математичні об'єкти: передбачається, що вони реалізуються всередині ідеального «чорного ящика», що забезпечує повну ізоляцію від зовнішнього середовища	Використовують інформацію про фізичні процеси в шифраторі, які не розглядаються в теоретичному описі криптографічного алгоритму. Важлива специфіка реалізації криптопримітивів: у програмі, на конкретному процесорі й т. ін.
Має велику загальність (не залежить від конкретної реалізації)	Мають меншу загальність, але в багатьох випадках можуть бути значно ефективнішими
Криптопримітиви обираються таким чином, щоб обчислювальна складність визначення їхніх секретних параметрів була максимальною	Поряд із побічними каналами, зумовленими специфікою реалізації криптосистеми, можливо цільове створення побічних каналів
Рівень безпеки криптосистеми оцінюється, з огляду на математичні властивості криптографічних алгоритмів і розмірів їхніх ключів	Рівень безпеки криптосистеми визначається тим, наскільки її реалізація відповідає характеристикам ідеального «чорного ящика»

Джерело: систематизовано авторами.

2. Можливості атак за побічними каналами. Бурхливий розвиток методів та практики SCA-атак у 90-х роках XX століття і на початку XXI століття виявив, що в багатьох випадках зловмисникам недоцільно намагатися подолати обчислювальну складність злому криптографічних примітивів, які використовуються в механізмах інформаційної безпеки, а вигідніше атакувати те обладнання криптосистеми (криптографічний модуль), де реалізовані криптографічні алгоритми.

При певних умовах SCA-атаки можуть бути значно ефективніші, ніж криптоаналітичні атаки, які базуються на звичайних методах математичного аналізу, і такі SCA-атаки набагато простіше реалізувати.

Стосовно SCA-атак, заснованих на вимірюванні часу виконання криптографічних операцій, досягнуто такі практичні показники [3]:

- для розкриття ключа алгоритму RSA (в режимі реалізації Монтгомері) довжиною 512 біт потребується від 5000 до 10000 вимірювань,
- ключ алгоритму RC5 можливо розкрити приблизно за 10^6 вимірювань,
- розкриття ключа алгоритму AES потребує порядку $4 \cdot 10^3$ вимірювань часу виконання певних процедур цього алгоритму.

За подібними показниками можливо реалізувати практичні атаки по часу також на алгоритми DES, IDEA та Open SSL [1].

Розроблено численні методи аналізу побічних каналів, які передбачають певну форму обробки цифрового сигналу та статистичні обчислення. Деякі з найважливіших методів включають простий аналіз потужності (SPA) [6], диференційний аналіз потужності (DPA) і кореляційний аналіз потужності (CPA).

Техніка SPA передбачає, що аналітик має на меті реконструювати секретний ключ, використовуючи лише одне трасування сигналу побічного каналу, і часто використовується різниця в базових операціях з елементами ключа, таких як подвійне додавання або додавання та множення. Проте SPA неможливий, якщо відношення сигнал/шум (SNR) недостатньо високе. У більшості випадків розроблені контрзаходи роблять SPA марним.

Методи DPA базуються на оцінці багатьох трасувань роботи цільового алгоритму із різними вхідними даними [6]. На їх основі може виконуватися атака, яка перевіряє гіпотези щодо елементів підключів для частини алгоритму (за методом «розділяй і володарюй»). Для DPA використовується велика кількість трасувань, щоб зменшити шум шляхом усереднення, і зазвичай застосовується однорозрядна модель потужності.

За певних умов застосування цих атак до алгоритму DES дозволяє розкривати як раундові ключі, так і невідомі бітові перестановки [3]. Для інших криптоалгоритмів можливо визначення операндів в операціях порівняння і множення, а також невідомого показника в операції обчислення модульної експоненти [3]. Поєднання таких атак з диференційним аналізом результатів вимірювань дозволяє проводити реверс-інжиніринг, тобто відновлення невідомих фрагментів криптоалгоритмів [3].

Іншим методом є кореляційний аналіз потужності (CPA), який застосовує багатобітну модель споживання потужності для зменшення впливу шуму на можливість виконання успішної атаки. Основна відмінність між цими двома методами полягає в тому, що DPA базується на обчисленні різниці між двома наборами трасувань, тоді як CPA використовує коефіцієнт кореляції для обчислення тесту залежності витоку даних про елементи секретного ключа від поведінки певних ознак у трасуваннях споживання потужності [7].

Вищевказані три методи атак за побічними каналами використовуються щодо широкого спектру криптографічних реалізацій.

Ще більш ефективними ніж DPA і CPA є атаки за шаблоном (Template Attacks – TA) [8], але вони вимагають етапу профілювання, тобто кроку, під час якого криптографічне обладнання знаходиться під повним контролем аналітика, щоб оцінити розподіл ймовірностей витоку інформації та краще використовувати всю інформацію, присутню в кожному трасуванні [8]. Етап профілювання може надати більш реальну статистичну модель процесів, які відбуваються під час роботи пристрою, замість використання якоїсь апріорної моделі. TA є найкращою (оптимальною) технікою з інформаційно-теоретичної точки зору, якщо аналітик має необмежену кількість трасувань, а розподіл шуму слідує закону Гаусса [9; 10].

Далі криптоаналітики з'ясували певні недоліки атак за шаблоном і спробували змінити їх, щоб краще впоратися з проблемами складності цих атак та їх переносу на інші реалізації. Прикладом такого підходу є атака за об'єднаним шаблоном, де використовується лише одна об'єднана коваріаційна матриця, щоб впоратися зі статистичними труднощами [11].

Крім таких спроб, спільнота криптоаналітиків з SCA виявила, що подібний підхід до профілювання використовується в інших сферах у формі керованого машинного навчання. Тому деякі дослідники почали експериментувати з різними методами машинного навчання (ML) і оцінювати їхню ефективність у контексті SCA. Розгляд різних сценаріїв та різних методів ML націлені на встановлення випадків використання, коли методи ML можуть перевершити атаку за шаблоном та стати найкращим вибором для етапу профілювання в SCA. Зокрема, у спільноті SCA показана актуальність методів глибокого навчання (DL), за допомогою яких отримуються значні результати в аналізі побічних каналів, навіть за наявності контрзаходів.

3. Особливості виконання атак з ін'єкції збоїв. Атаки з ін'єкції збоїв (або збурень) передбачають активне маніпулювання чипом криптомодуля, щоб викликати тимчасову помилку під час виконання певного процесу. Мета полягає в тому, щоб обійти захист її конфіденційних активів. Наприклад, помилка може дозволити обійти перевірку умов безпеки, як-от перевірку правильності PIN-коду.

Є кілька методів викликання збоїв при обчисленнях. За допомогою неінвазивних атак можливо виконання збоїв тактових імпульсів або напруги живлення [12]. Смарткартки користуються зовнішнім джерелом живлення і тактових імпульсів. В обох цих випадках при застосуванні параметрів живлення та частоти імпульсів поза межами робочих діапазонів можуть виникати збої в процесах, які виконуються на картці.

Під час повністю інвазивних атак відбувається активна інжекція дефекту за допомогою мікрозондування [13]. Для цього потрібно певним чином підготувати чип: декапсулювати чип, зняти шар пасивації та обійти екранування. Хоча таке можливо, але це дуже трудомісткий процес [14]. Через вартість цього методу та необхідних інструментів – це не вважається практичним шляхом атаки.

Проте ін'єкція оптичного збою вимагає лише мінімальної підготовки чипу: потрібно отримати доступ до передньої або задньої сторони чипу. Це можна зробити шляхом декапсуляції або видалення контактної панелі смарткартки. Для новітніх захищених мікроконтролерів вартість зростає через вищі вимоги до точності таких маніпуляцій. Однак, з точки зору витрат часу і грошових витрат, це все ще цілком можливо для достатньо оснащеного аналітика.

а) Збурення напруги живлення та тактової синхронізації. При збуренні тактової синхронізації пристрою його робота тимчасово прискорюється шляхом введення одного або кількох коротких імпульсів, що подаються на смарткарту від зовнішнього генератора. Це призводить до можливого внесення помилки у виконання інструкції. Наприклад, коли ЦП зчитує під час збою комірку пам'яті, то результат може бути зчитаний до того, як дані стануть стабільними на шині пам'яті. Це призводить до отримання неправильного значення. Подібним чином збій напруги живлення під час виконання інструкції читання може призвести до зчитування неправильних значень із пам'яті.

Інший ефект, який може виникнути, полягає в тому, що інструкція вибирається з пам'яті, але її виконання не завершується: пришвидшення тактових імпульсів може викликати наступну інструкцію, яка вже вибрана з пам'яті.

б) Ін'єкція оптичних збоїв. Оптичні збої виникають під впливом сильного джерела світла, наприклад, фотоспалаху або лазерного променю [15]. Оскільки напівпровідники за своєю природою чутливі до світла, можна перемикати транзистори за допомогою

оптичного імпульсу. Використовуючи прецизійну платформу позиціонування і сфокусований лазерний промінь, можна точно націлитися на певні ділянки мікросхеми. Хоча це створює додаткові труднощі стосовно двовимірного пошуку (координат X і Y) потрібної ділянки, це дозволяє дуже конкретно зосередитися, наприклад, на декодери пам'яті, ЦП або компонентах криптографічного алгоритму. Таким чином можна уникати спрацювання механізмів протидії втручанням у роботу чипу, заснованих на використанні в мікросхемі світлочутливих елементів. У цьому сенсі розмір плями та довжина хвилі фотонів є також важливими параметрами.

З погляду підготовки кристал чипа повинен бути оптично експонований (оголений, доступний для оптичного впливу). Передня сторона містить шар(и) транзисторів і металевих з'єднань, які покриті епоксидною смолою. Ця сторона зазвичай вимагає видалення цієї епоксидної смоли (декапсуляції), хоча для деяких чипів навіть це не є обов'язковим, оскільки часто використовується прозора епоксидна смола. Тильна сторона чипу – це сторона підкладки, яка для забезпечення оптичного доступу до кристалу мікросхеми зазвичай потребує видалення центральної частини контактної панелі смарткартки. Іноді для отримання доступу потрібна декапсуляція та повторне перепаювання контактної панелі.

Через потребу зазначеної мінімальної підготовки чипу, ін'єкція оптичного збою вважається напівінвазивною атакою. Попри цей недолік, метод є найуспішнішою атакою зі збурення смарткарти, оскільки контрзаходи проти неї, як вказано вище, нелегко реалізувати.

в) Застосування атак з ін'єкції збоїв. Ін'єкція збоїв може використовуватися для досягнення різних ефектів: обходу механізму розділення доступу, дампу захищеної пам'яті, обнуління (часткове) ключа, диференційного аналізу помилок (DFA) та заходів впливу на реалізовані в чипі механізми протидії аналізу побічних каналів. Обхід розділення доступу досягається, коли криптоаналітик порушує уразливе для доступу рішення (наприклад, результат автентифікації), що призводить до збільшення привілеїв. З цими привілеями зловмисник може отримати доступ до конфіденційних даних. Прикладом може бути порушення верифікації PIN-коду, після чого банківська картка підписуватиме запити на транзакцію.

Щоб отримати дамп пам'яті, криптоаналітик збурює пристрій під час передачі даних. Через збурення дані передаються з неправильного місця пам'яті або видається зайва кількість даних. В обох випадках може статися витік конфіденційних даних. Старіші смарт-карти іноді були вразливі до цієї атаки під час передачі своїх команд ATR, що в крайніх випадках призводило до повних дампів пам'яті.

Часткове обнуління ключа – це атака, за допомогою якої зловмисник встановлює частину секретного ключа на всі 0-ві біти (або на всі «1») і не впливає на кілька байтів ключа. Знаючи змінену частину ключа, ці кілька байтів, що не змінилися, можна розкрити методом тотального випробування, якщо відомі вхідні та вихідні дані. Повне обнуління ключа може бути доцільним при атаках на протоколи, що використовують секретний ключ: якщо секретний ключ використовується, наприклад, для автентифікації, то примусове присвоєння ключу відомого значення дозволяє протоколу автентифікації успішно працювати без знання фактичного секретного ключа.

Диференціальний аналіз помилок (DFA) можна виконати після порушення криптографічної операції, що призведе до пошкодження підписів або криптограм. За допомогою математичного аналізу ці пошкоджені дані можна використати для вилучення секретного або приватного ключа. Прикладом DFA з однією помилкою є атака RSA/CRT «Bellcore» [16], яка дозволяє отримати повний приватний показник RSA з одного помилкового обчислення. Інші атаки дозволяють отримувати ключі ряду асиметричних і симетричних алгоритмів шифрування, включаючи DES і AES [17].

Виробники пристроїв криптографічного захисту інформації знають про загрози атак з ін'єкції збоїв і зазвичай впроваджують низку контрзаходів для пом'якшення ризиків. Тому вважається, що більшість сучасних захищених мікроконтролерів мають належний захист від певних типів таких атак. Діапазон параметрів для належної роботи цих контролерів чітко визначений [19] і може бути перевірений самою мікросхемою. Захищені мікроконтролери також виконують більшість своїх операцій на основі внутрішнього генератора тактових імпульсів, і тому вони не настільки чутливі до зовнішніх збурень тактової синхронізації, як мікроконтролери, що працюють від зовнішнього генератора тактових імпульсів.

Контрзаходи зосереджені як на запобіганні збоїв шляхом фільтрації вхідних даних, так і на їх виявленні шляхом постійного моніторингу відповідних інтерфейсів. Якщо виявлено введення вхідних даних, що не відповідають специфікаціям, карта може певним чином відреагувати на цю подію.

Водночас зловмисники вдосконалюють методи атаки, щоб кинути виклик цим контрзаходам, що призводить до певної «взаємодії» сторін, яка просуває процес постійного покращення безпеки карток.

Однак зловмисник завжди може покращити ефективність аналізу побічних каналів шляхом впливу на контрзаходи проти DPA та CPA [20]. Подібним чином, за допомогою ін'єкції збоїв у потрібний час можна вимкнути або вплинути на контрзаходи проти збурення. Деякі контрзаходи мають параметри налаштування, які встановлюються в певний момент під час завантаження карти. За допомогою ін'єкції збоїв можна пропустити їх увімкнення або, наприклад, порушити баланс генераторів випадкових чисел.

4. Особливості забезпечення інформаційної безпеки під час реалізації криптографічних алгоритмів.

В аспекті інформаційної безпеки обчислювальних і комунікаційних систем практична загроза SCA- та FI-атак потребує такої реалізації криптографічних алгоритмів, щоб у процесі обчислень під час виконання цих алгоритмів дані секретного ключа не розкривалися, незважаючи на можливості зловмисника спостерігати і маніпулювати процесом виконання алгоритму.

Існує декілька підходів щодо реалізації цієї вимоги.

Перший підхід полягає в застосуванні Загальних Критеріїв оцінки захищеності інформаційних технологій (Common Criteria for Information Technology Security Evaluation, [4]) – міжнародного стандарту, що описує інфраструктуру, у якій користувачі системи, яка розроблюється, можуть описати вимоги, розробники можуть заявити про властивості безпеки системи, які можуть гарантувати, а експерти з безпеки визначити, чи задовольняє отримана система заявам. Таким чином забезпечуються умови, у яких процес опису, розробки та перевірки інформаційної безпеки буде проведений із необхідною скрупульозністю.

Другий підхід забезпечує кількісне визначення рівня безпеки при оцінці інформаційної захищеності системи в межах сценарію, наведеного на рис. 2. Це реалізовано, наприклад, в стандарті для федеральних органів США FIPS 140-2 (Federal Information Processing Standard, [1]), який визначає специфікації побудованих на основі криптографії систем безпеки, призначених для захисту конфіденційних або цінних даних щодо забезпечення конфіденційності й цілісності такої інформації. Стандарт FIPS 140-2 визначає вимоги, яким повинні задовольняти криптографічні модулі відповідно до чотирьох якісно різних рівнів безпеки: від низького рівня 1 до високого рівня 4.

Третій підхід, звичайно, реалізується у військовій сфері. Він полягає в застосуванні для захисту військового електронного обладнання стандартів TEMPEST (Transient Electromagnetic Pulse Emanation Standard, [5]), які гарантують неможливість витоку корисної інформації шляхом паразитних радіовипромінювань, через лінії електропередач або інші випромінювання.

Разом з тим, застосування цих підходів не надає гарантованого захисту від SCA-атак. Стандарт FIPS 140-2, наприклад, має справу тільки зі специфікаціями щодо пом'якшення впливу атак, для яких нині немає перевірених заходів запобігання. На практиці, можуть бути знайдені або створені нові побічні канали витоку й може бути отримана побічна інформація для криптоаналізу.

Висновки. Незважаючи на наявність та використання у світі стандартизованих підходів з забезпечення інформаційної безпеки, стурбованість, що пов’язана із застосуванням SCA- та FI-атак, з порядку денного не знімається.

Для розвинутої держави, яка претендує на свій цифровий суверенітет, нагальною необхідністю є підготовка фахівців у галузі методології та застосування SCA-атак, – як для розуміння їхніх практичних можливостей щодо порушення інформаційної безпеки обчислювальних і комунікаційних систем, так і в аспекті аналізу методів і прийомів зазначених атак для створення нових систем протидії, які реально підвищують рівень інформаційної безпеки.

Список використаних джерел

1. Zhou, Y. B. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing [Electronic resource] / Y. B. Zhou, D. G. Fen // Information Security Seminar WS 0607. – 2006. – Access mode: https://eprint.iacr.org/2005/388.pdf.

2. Cryptographic processors – a survey / R. Anderson, M. Bond, J. Clulow, S. Skorobogatov // Proceedings of the IEEE. – 2006. – Vol. 94, fasc. 2. DOI: 10.1109/JPROC.2005.862423.

3. Quisquater, J.-J. Side Channel Attacks. State-of-the-art [Electronic resource] / J.-J. Quisquater, F. Koeune. – Access mode: https://www.cryptrec.go.jp/exreport/cryptrec-ex-1047-2002.pdf.

4. ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security [Electronic resource]. – Access mode: www.tools.commoncriteria.pl/ccHelp.

5. SST TEMPEST Introduction iss 3 [Electronic resource]. – Access mode: https://www.giac.org/paper/gsec/4287/tempest-electromagnetic-emanations-security-government-standard/106943, September 2023.

6. Kocher, P. C. Differential power analysis. In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology / P. C. Kocher, J. Jaffe, B. Jun // CRYPTO ’99. – London : Springer-Verlag, 1999. – P. 388-397.

7. Brier, É. Correlation Power Analysis with a Leakage Model / É. Brier, C. Clavier, F. Olivier. // CHES (Cambridge, August 11-13, 2004). – Springer, 2004. – Vol. 3156 of LNCS. – P. 16-29.

8. Chari, S. Template Attacks / S. Chari, J. R. Rao, P. Rohatgi // CHES (San Francisco Bay (Redwood City), August 2002). – Springer, 2002. – Vol. 2523 of LNCS. – P. 13-28.

9. Heuser, A. Good is Not Good Enough — Deriving Optimal Distinguishers from Communication Theory / A. Heuser, O. Rioul, S. Guilley // CHES. – 2014. – Vol. 8731 of LNCS.

10. Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis) / L. Lerman, R. Poussier, G. Bontempi, O. Markowitch, F.-X. Standaert // Constructive Side-Channel Analysis and Secure Design : 6th International Workshop 252 References COSADE 2015 (Berlin, April 13–14, 2015). Revised Selected Papers. – Springer, 2015. – Vol. 9064 of LNCS. – P. 20-33.

11. Choudary O. Efficient template attacks. / O. Choudary, M. G. Kuhn // Smart Card Research and Advanced Applications : 12th International Conference, CARDIS 2013 (Berlin, November 27-29, 2013). Revised Selected Papers. – Springer, 2013. – Vol. 8419 of LNCS. – P. 253-270.

12. A Taxonomy of Side Channel Attacks on Critical Infrastructures and Relevant Systems / N. Tsalis, E. Vasilellis, D. Mentzelioti, T. Apostolopoulos // Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. – Springer, 2019. https://doi.org/10.1007/978-3-030-00024-0_15.

13. Joint Interpretation Library, Application of Attack Potential to Smartcards [Electronic resource]. – Version 2.7. – JIL Hardware Attacks Subgroup, 2009. – Access mode: https://sogis.eu/documents/cc/domains/hardware_devices/poi/JIL-Application-of-Attack-Potential-to-POIs-v1-0_2011_06_09-for_trial_use.pdf.

14. Gupta H. Impact of Side Channel Attack in Information Security / H. Gupta // 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). – Dubai, 2019. – P. 291-295. DOI: 10.1109/ICCIKE47802.2019.9004435.

15. Boneh, D. On the Importance of Eliminating Errors in Cryptographic Computations / D. Boneh, R. A. DeMillo, R. Lipton // Journal of Cryptology. – 2001. – № 14(2). – P. 101-120.

16. Biham, E. Differential cryptanalysis of the data encryption standard / E. Biham, A. Shamir // Advances in Cryptology – CRYPTO ’97 : 17th Annual International Cryptology Conference. – LNCS, 1997. – Vol. 1294. – P. 513-525.

17. Practical Fault Attack on a Real-World ECC Library / L. Batina, M. M. Lauridsen, E. Markovski, P. K. Larsen // Cryptographic Hardware and Embedded Systems. – Amsterdam, 2018.

18. ISO/IEC 7816-3:2006. Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols [Electronic resource]. – Access mode: https://www.en-standard.eu/bs-iso-iec-7816-3-2006-identification-cards-integrated-circuit-cards-cards-with-contacts-electrical-interface-and-transmission-protocols/?gad_source=1&gclid=CjwKCAiA-vOsBhAAEiwAIWR0TaqrPeVx1_U42rfxlffbryuSiy9Iym9VR3v4SwYEMUAUIdzua3ie7RoClbQQAvD_BwE.

19. Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis [Electronic resource] / F. Amiel, K. Villegas, B. Feix, L. Marcel – Vienna : FDTC, 2007. – 20 p. – Access mode: https://fdtc.deib.polimi.it/FDTC07/Feix.pdf.

References

1. Yong Bin Zhou, Deng Guo Fen. (2006). Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. *Information Security Seminar WS 0607*.

2. Anderson, R., Bond, M., Clulow, J., Skorobogatov, S. (2006). Cryptographic processors – a survey. *Proceedings of the IEEE*, 94, fasc. 2. DOI:10.1109/JPROC.2005.862423.

3. Jean-Jacques Quisquater, Francois Koeune. (2002). *Side Channel Attacks. State-of-the-art*. https://www.cryptrec.go.jp/exreport/cryptrec-ex-1047-2002.pdf.

4. ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security. www.tools.commoncriteria.pl/ccHelp.

5. SST TEMPEST Introduction iss 3. https://www.giac.org/paper/gsec/4287/tempest-electromagnetic-emanations-security-government-standard/106943.

6. Paul C. Kocher, Joshua Jaffe, & Benjamin Jun. (1999). Differential power analysis. In Proceedings of the *19th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO’99* (pp. 388–397). Springer-Verlag.

7. Éric Brier, Christophe Clavier, & Francis Olivier. (August 11–13 2004). Correlation Power Analysis with a Leakage Model. *CHES*, *3156 of LNCS*, 16–29.

8. Suresh Chari, Josyula R. Rao, & Pankaj Rohatgi. (August 2002). Template Attacks. In *CHES, 2523 of LNCS*, 13–28. Springer. San Francisco Bay (Redwood City), USA.

9. Annelie Heuser, Olivier Rioul, & Sylvain Guilley. (2014). Good is Not Good Enough – Deriving Optimal Distinguishers from Communication Theory. In *Lejla Batina and Matthew Robshaw, editors, CHES, 8731 of Lecture Notes in Computer Science*.

10. Liran Lerman, Romain Poussier, Gianluca Bontempi, Olivier Markowitch, & François-Xavier Standaert. (April 13–14, 2015). Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis). In Stefan Mangard, Axel Y. Poschmann (ed.), *Constructive Side-Channel Analysis and Secure Design - 6th International Workshop,252 References COSADE 2015*. Berlin, Germany. Revised Selected Papers, volume 9064 of Lecture Notes in Computer Science (pp. 20–33).

11. Omar Choudary, & Markus G. Kuhn. (November 27–29, 2013). Efficient template attacks. In Aurélien Francillon and Pankaj Rohatgi (ed.), *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013*. Berlin, Germany,. Revised Selected Papers, volume 8419 of LNCS (pp. 253–270).

12. Tsalis, N., Vasilellis, E., Mentzelioti, D., Apostolopoulos, T. (2019). A Taxonomy of Side Channel Attacks on Critical Infrastructures and Relevant Systems. In Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds.), *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham. https://doi.org/10.1007/978-3-030-00024-0_15.

13. JIL Hardware Attacks Subgroup, “Joint Interpretation Library, Application of Attack Potential to Smartcards”, Version 2.7, Februari 2009.

14.Gupta H. et al. (2019). Impact of Side Channel Attack in Information Security. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Dubai, United Arab Emirates (pp. 291-295). DOI: 10.1109/ICCIKE47802.2019.9004435.

15.Boneh D., DeMillo R. A., Lipton R. (2001). On the Importance of Eliminating Errors in Cryptographic Computations. *Journal of Cryptology, 14*(2), 101–120.

16.Eli Biham, Adi Shamir (1997). Differential cryptanalysis of the data encryption standard. *Advances in Cryptology – CRYPTO '97: 17th Annual International Cryptology Conference, LNCS*, *1294,* 513-525.

17.Batina L., Lauridsen M. M., Markovski E., Larsen P. K. (2018). Practical Fault Attack on a Real-World ECC Library. *Cryptographic Hardware and Embedded Systems*. Amsterdam, Netherlands.

18."Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols", ISO/IEC 7816-3:2006.

19.Amiel F., Villegas K., Feix B., Marcel L. (2007). *Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis.* FDTC.

Отримано 11.12.2023

UDC 004.056.53

Anatoly Boroda[1], Taras Petrenko[2]

[1]PhD in Technical Sciences, Chief Researcher of the Research Department of the Research Center
State Research Institute of Cyber Security Technologies and Information Protection (Kyiv, Ukraine)
E-mail: anv_boroda@ukr.net. **ORCID:** https://orcid.org/0009-0007-9302-8297. **ResearcherID:** JRX-2757-2023
[2]PhD in Technical Sciences, Associate Professor of the Department of Cyber Security and Mathematical Modeling
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: mail_taras@stu.cn.ua. **ORCID:** https://orcid.org/0000-0001-5571-3815. **ResearcherID:** G-5801-2014

IMPACT OF ATTACKS THROUGH SIDE CHANNELS ON INFORMATION SECURITY

The main structural elements of security mechanisms based on cryptography are cryptographic primitives, namely cryptographic algorithms - symmetric ciphers, public key ciphers and hash functions, which are used to implement the necessary functions of the security mechanism. In order for the cryptographic system to ensure information security, it is necessary that the secret keys used in the cryptographic algorithms for security implementation remain secret (not revealed) under any circumstances. However, in practice, the implementation and operation of cryptographic security mechanisms is far from the perfection of an ideal "black box". That is why side channel attacks are a serious threat to the security of cryptographic modules and, as a result, to the information security of computing and communication systems. Therefore, when implementing protection mechanisms, all possibilities of such attacks should be evaluated and all aspects of their application should be taken into account.

The analysis of scientific works in the field of protection of cryptographic systems against attacks by side channels proved that these issues are not given enough attention today.

The purpose of the article is the study of attacks through side channels on the implementation of crypto-protection mechanisms, the analysis of the features of their implementation, and an overview of the mechanisms for ensuring information security during the destructive effects of these attacks.

The paper considers one of the practical directions of cryptanalysis - attacks through side channels on the implementation of crypto-protection mechanisms. The differences between theoretical cryptanalysis and side-channel attacks are studied. The possibilities of side-channel attacks and the specifics of failure injection attacks are analyzed. The features of ensuring information security during the implementation of cryptographic algorithms for protection against side channel attacks are considered. The need to take into account the threat of these attacks when ensuring the information security of computer and communication systems is proven.

Keywords: *side channel attacks; cryptosystem; information security.*

Fig.: 2. References: 19.

Бородa А., Петренко Т. Вплив атак за побічними каналами на інформаційну безпеку. *Технічні науки та технології.* 2023. № 4(34). С. 91-103.