УДК 003.26:004.056.55:621.39

[1]О.Г. Корченко , д.т.н.
[2]Є.В. Васіліу, к.ф.-м.н.
[1]С.О. Гнатюк
[1]В.М. Кінзерявий

АТАКИ В КВАНТОВИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

[1]Національний авіаційний університет, e-mail: s.gnatyuk@nau.edu.ua
[2]Одеська національна академія зв'язку ім. О.С. Попова, e-mail: vasiliu@ua.fm

У даній статті запропонована розширена класифікація атак у квантових системах захисту інформації, яка враховує як атаки на квантові підсистеми розподілу ключів та прямого безпечного зв'язку, так і атаки на класичні підсистеми шифрування. Це дасть можливість формалізувати напрямки подальших досліджень щодо розробки ефективних систем захисту інформації.

Вступ

На даний момент з усіх існуючих квантових технологій захисту інформації (ЗІ) [1, 2] лише системи на основі квантового розподілу ключів (КРК) є реалізованими практично, як окремі модулі та компоненти, інтегровані в існуючі інформаційно-комунікаційні системи (ІКС). Системи КРК мають безумовну стійкість [3], що забезпечується законами квантової фізики і якщо будь-яку з них об'єднати з криптосистемою, яка теж матиме безумовну стійкість (на сьогодні така стійкість доведена лиш для схеми шифрування Вернама), то отримаємо безумовно стійку систему шифрування даних. Фундаментальні закони квантової механіки [3, 4] з одного боку забезпечують виявлення атаки пасивного перехоплення, а з іншого – допускають можливість реалізації різного роду атак у квантових системах захисту інформації (КСЗІ). Зважаючи на те, що у квантовому каналі неможливо відрізнити природні завади від тих, що створюються зловмисниками при спробі підслуховування, необхідно передбачити цей факт при проектуванні превентивних систем.

Аналіз існуючих досліджень

У роботі [5] проведено якісний аналіз атак у кіберпросторі (cyber space), а праця [6] містить розширену класифікацію кібератак (cyber attack) за ознаковим принципом. Крім того, у роботі [7] наведена класифікація атак на канали КРК: виділено два класи таких атак – це атаки на кубіти та атаки, що використовують неідеальність компонентів системи. У роботі [8] проаналізована атака на протокол BB84 у припущенні, що криптоаналітик може управляти ймовірностями вибору базисних векторів для виміру станів кубітів, а також одночасною зміною базисів відправника й адресата. Базова класифікація атак на КРК за критерієм складності необхідного для проведення атаки обладнання наведена у [3, 4, 9]. Зважаючи на те, що системи КРК нерозривно пов'язані та практично використовуються у комплексі із класичними шифрувальними сегментами, то виникає потреба розширення існуючих класифікацій шляхом включення криптоаналітичних атак (cryptanalytic attack) на шифрувальні модулі. Така узагальнена класифікація на даний момент відсутня у науковій літературі, як і класифікація атак на інші КСЗІ, крім КРК (зокрема на системи квантового прямого безпечного зв'язку (КПБЗ)). Таким чином, виникають труднощі при побудові моделі порушника (attacker model) у КСЗІ та оцінці можливостей таких систем протидіяти зловмисникам. ***Метою*** даної статті є розширення класифікації атак, а також побудова моделі порушника у КСЗІ. Реалізація поставленої мети дозволить формалізувати напрямки подальших досліджень щодо розробки та побудови ефективних систем ЗІ на основі квантових технологій.

На рис. 1 наведена загальна класифікація атак у КСЗІ.

Загальна класифікація атак за ступенем складності

На основі [1–4, 7–9] можна ввести наступне визначення – *атаками у КСЗІ* називаються заходи, які застосовуються для підриву безпеки даних систем чи реалізації загроз базовим характеристикам безпеки (конфіденційності, цілісності, доступності) систем квантової криптографії (КК) шляхом використання їх уразливостей. Як згадувалось раніше, ціллю атак у КСЗІ можуть бути підсистеми КРК і підсистеми безпосереднього шифрування даних (ПШД). При використанні легітимними користувачами *ідеальних однофотонних джерел*, атаки в

системах КК (за ступенем складності) можна умовно поділити на *когерентні* та *некогерентні*. У свою чергу, некогерентні (індивідуальні) атаки [4, 9, 10] бувають *непрозорими* (*opaque attacks*) та *напівпрозорими* (*semi-translucent attacks*). Непрозорі атаки (їх також називають *атаками "перехоплення – повторної посилки кубітів", intercept-resend attack* [4]) полягають у вимірюванні зловмисником (Євою) безпосередньо квантового стану носія (фотона) і подальшій повторній посилці нового фотона у стані, який отримано в результаті вимірювання. Оскільки зловмисник не пропускає квантові стани відправника (Аліси), а генерує нові і відправляє їх приймаючій стороні (Бобові), то даний клас атак називається непрозорим.

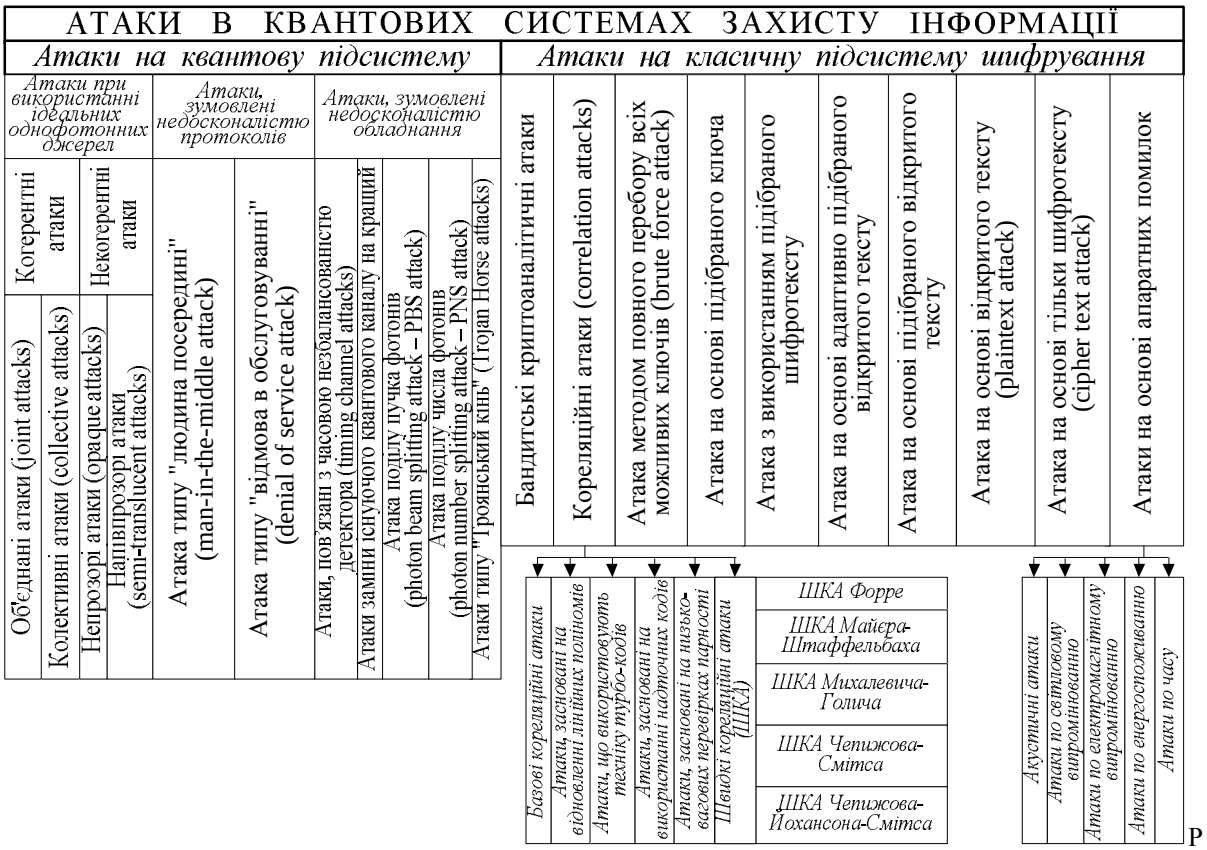

Рис.1. Розширена класифікація атак у КСЗІ

Напівпрозорі атаки [4, 9] передбачають використання Євою допоміжних квантових систем (квантових проб – КП) для переплутування (entanglement) їх з носіями, які Аліса пересилає Бобу через квантовий канал. Після взаємодії, передавані та допоміжні стани знаходяться у загальному переплутаному стані, потім перші передаються Бобові, а другі зберігаються у квантовій пам’яті у Єви. Після закінчення відкритого обміну інформацією між Алісою та Бобом на етапі просіювання ключа, зокрема об'явлення базисів, в яких Боб вимірював фотони Аліси, Єва визначає послідовність базисів, яку необхідно використати для вимірювання станів її проб, щоб отримати якомога більше інформації про ключ. Стани фотонів Аліси змінюються після переплутування з пробами Єви, проте рівень помилок при даній атаці значно нижчий, ніж при непрозорій атаці. Варто відмітити, що для реалізації подібної атаки Єві необхідно мати квантову пам'ять (quantum memory) великого обсягу для зберігання проб до об’явлення базисів Бобом, та складне обладнання для переплутування проб з фотонами Аліси. Напівпрозорі атаки є також одним з основних видів атак на КПБЗ. У роботі [11] розглядається атака з використанням КП на пінг-понг протокол КПБЗ з ГХЦ-триплетами [3], а також обчислено повну ймовірність виявлення атаки зловмисника в залежності від кількості отриманої ним інформації для трьох варіантів пінг-понг протоколу. Доведено, що інформаційна місткість (information capacity) та стійкість різних варіантів даного протоколу є обернено пропорційними величинами. При цьому, якщо Єва вибере атаку, яка дає повну інформацію про передані біти, протокол з парами Белла і надщільним кодуванням (superdense coding) та протокол з ГХЦ-триплетами мають практично однаковий рівень стійкості до некогерентної атаки.

При когерентних атаках [3, 4, 9, 10, 12] Єва може будь-яким (унітарним) способом переплутати пробу будь-якого розміру з групою передаваних фотонів. Одним із підвидів даного класу атак є *колективна атака* (*collective attack*) [3, 9, 10]. Дана атака схожа з напівпрозорою в начальній стадії, тобто кожній фотон Аліси індивідуально переплутується з окремою пробою. Отже, Єва отримує проби в таких же станах, як і при напівпрозорій атаці. Але після закінчення відкритого обміну інформацією між Алісою та Бобом, Єва виконує вимірювання відразу на всіх КП, як на єдиній квантовій системі. Найефективнішою є *об'єднана атака* (*joint attack*) [4, 9] – це окремий випадок когерентної атаки, при якій Єва використовує єдину КП (з гільбертового простору станів більшої розмірності) для переплутування з усією послідовністю фотонів, що Аліса передає Бобові. Але ця атака є також і найбільш складною з технічної точки зору. Підводячи підсумки, варто було б відзначити, що відповідно до сучасного рівня техніки реалізація когерентних атак не є можливою (на відміну від некогерентних атак), так як на сьогодні не існує необхідних квантової пам'яті великого обсягу та багатокубітного квантового комп'ютера (many-qubit quantum computer).

Атаки, зумовлені недосконалістю протоколів

Недосконаліть протоколів є серйозним чинником для реалізації атак в системах КК. Найвідомішими атаками цього класу є *атака "людина посередині"* (*man-in-the-middle attack*) та *атака "відмова в обслуговуванні"* (*denial of service attack*). Для атаки "людина посередині" Єва має повністю контролювати класичний канал зв'язку між Алісою та Бобом, тобто мати можливість замінювати усі повідомлення, що передаються класичним каналом. Варто відзначити, що усі існуючі протоколи КРК і КПБЗ є вразливими до даної атаки [2]. Захист від такої атаки є загальновідомим – аутентифікація легітимних користувачів у класичному каналі.

Що стосується атаки "відмова в обслуговуванні", то вперше для оригінального пінг-понг протоколу КПБЗ така атака була розглянута в роботі [13]. Суть її полягає у тому, що Єва не переплутує свою пробу з кубітом на шляху від Боба до Аліси, а просто вимірює стан кубіта на зворотному шляху від Аліси до Боба (в режимі передачі повідомлення) – цим самим порушуючи взаємну кореляцію (mutual correlation) кубітів Аліси та Боба. У результаті Єва не отримає ніякої корисної інформації, проте зруйнує квантовий канал між Алісою та Бобом. У випадку ГХЦ-триплетів Єва може також вимірювати стани одного чи двох кубітів і порушувати таким чином переплутаність стану триплету [11]. Відзначимо, що до атаки "відмова в обслуговуванні" також вразливі практично всі протоколи КК.

Атаки, зумовлені недосконалістю обладнання

У класичній криптографії атаки, зумовлені недосконалістю обладнання, називають також *атаками, що використовують витік інформації побічними каналами* (*side-channel attacks*). Атаки такого типу можливі також і в КК.

Атаки типу "Троянський кінь" (*Trojan Horse attack*). До атак даного типу уразливі так звані двосторонні (two-way) протоколи КРК та КПБЗ, тобто протоколи, в яких фотони пересилаються від Боба до Аліси та назад від Аліси до Боба. Прикладом такого протоколу є вищезгаданий пінг-понг протокол КПБЗ. Вперше атака типу "троянський кінь" була запропонована в [4]. Єва посилає світлові імпульси у квантовий канал, що з'єднує апаратуру Аліси та Боба, і потім аналізує відбите світло. Таким способом у принципі можливо виявити, який лазер або який датчик тільки що спрацював, або параметри настроювання модуляторів поляризації й фази. Така атака не може бути просто відвернена використанням засувки, тому що Аліса та Боб повинні залишити "двері відкритими" для своїх фотонів. Але Аліса й Боб могли б виявити додаткові фотони Єви, так як при такій атаці відбувається збільшення енергії імпульсів. Тому Єва повинна використовувати світло іншої довжини хвилі, ніж використовують Аліса та Боб, а саме такої довжини хвилі, до якої датчики Аліси й Боба є нечутливими [4]. Інший спосіб для Єви приховати атаку полягає в тому, що вона перехоплює сигнал, переданий від Боба до Аліси, і потім вставляє додатковий фотон у сигнал з часом затримки, коротшим ніж часове вікно датчика [4, 14]. Таким чином, Аліса не може виявити цей додатковий фотон, оскільки він не спричинює спрацювання її датчика. Після кодувальної операції, яку виконує Аліса, Єва перехоплює сигнал знову й відокремлює додатковий фотон. Вона може одержати повну інформацію про кодувальну операцію Аліси, виконавши відповідне вимірювання. Такий варіант атаки отримав назву *атаки*

"троянського коня з затримкою фотона" [14]. Для протидії атаці "Троянський кінь" з використанням фотонів інших довжин хвиль, ніж використовують Аліса та Боб, вони повинні встановити фільтр сигналів з іншими довжинами хвиль на вході свого обладнання [4, 14, 15]. На практиці Аліса й Боб повинні експлуатувати фільтр довжини хвилі для фільтрування фонового світла, особливо коли у якості квантового каналу використовується вільний простір (бездротовий оптичний канал). Таким чином, немає проблеми для легітимних користувачів запобігти такій атаці [4]. Для атаки "троянського коня з затримкою фотона" Аліса повинна використовувати світлодільник 50/50 [14], щоб розділити кожний сигнал на дві частини й провести вимірювання їх станів у двох вимірювальних базисах. Якщо є тільки один фотон в оригінальному сигналі, то спрацює лише один з датчиків, інакше – спрацюють обидва. Таким чином, атаки типу "Троянський кінь" можуть бути відвернені технічними засобами. Але той факт, що цей клас атак існує, ілюструє, що безпека КК не може гарантуватися тільки принципами квантової механіки, але обов'язково покладається також на технічні засоби [4].

Атака поділу числа фотонів (*photon number splitting attack – PNS attack*). Найпростішим видом знімання інформації у звичайних оптичних телекомунікаційних системах є розділення пучка фотонів. Однак у протоколах КК передача повинна відбуватися за допомогою одиночних фотонів і, в такому випадку, Єва не може відвести частину сигналу. Тому даний вид атак неможливо провести у системах КК в ідеальних умовах однофотонних імпульсів (ОФІ). Але такі джерела сигналів поки не створені. На практиці в системах КРК використовують слабкі когерентні імпульси, випромінювані лазерними світлодіодами [2]. Число фотонів в імпульсі визначається розподілом Пуассона, тобто частина переданих імпульсів містить два й більше фотони. Таким чином, на практичні системи КРК, які використовують протокол BB84, стає можливим атака поділу числа фотонів [2, 16–18]. Для проведення такої атаки для кожного імпульсу, що посилається Алісою, Єва повинна виконати квантове неруйнуюче вимірювання числа фотонів в імпульсі, не впливаючи при цьому на їхню поляризацію. Відзначимо, що таке вимірювання дуже складно виконати, але на теперішній час це технічно можливо [17]. Якщо Єва виявляє в імпульсі більше одного фотона, вона відводить один, дозволяючи іншим безперешкодно пройти до Боба. Потім Єва виконує переплутування перехопленого фотона зі своєї пробою і очікує, коли після завершення передавання легітимні сторони оголосять використані базиси. Виконуючи потім вимірювання стану проби, Єва одержує точне значення переданого біта, не вносячи при цьому ніяких помилок у просіяний ключ, тобто атака Єви залишається невиявленою. Якщо ж імпульс несе один фотон, то стратегії Єви можуть бути різними. Наприклад, вона може просто пропускати всі ОФІ, що дозволить їй залишитися невиявленою. Однак при малому середньому числі фотонів в імпульсі (на практиці обладнання настроюють так, щоб це число було порядку 0,1) кількість багатофотонних імпульсів (БФІ) буде невеликою, і це не дозволить Єві одержати будь-яку суттєву інформацію про ключ. Інша стратегія полягає у тому, що Єва виконує некогерентну атаку на ОФІ. У цьому випадку, зрозуміло, вона вносить помилки в просіяний ключ, кількість яких буде залежати як від типу атаки, так і від частки ОФІ при передачі ключа.

Ще одна стратегія Єви полягає у блокуванні частини ОФІ – у результаті Боб одержує порожній імпульс, тобто його датчик не реєструє фотон. Таким блокуванням частки ОФІ Єва збільшує частку БФІ, що дозволяє їй збільшити інформацію про ключ при тому ж рівні внесених у просіяний ключ помилок. Оскільки чутливість сучасних датчиків, які використовуються в комерційних системах КРК, невелика, і вони реєструють в середньому лише 20–30% одиночних фотонів, а крім цього також відбуваються втрати фотонів в каналі, то Єва теоретично може таким чином приховати свою атаку. Але Боб, знаючи ймовірність одержати порожній імпульс при наявному обладнанні, може виявити значне перевищення кількості порожніх імпульсів над очікуваним. Відзначимо, що Боб може також не тільки визначати кількість порожніх імпульсів, але й контролювати всю статистику одержуваних ним сигналів, виконуючи неруйнуюче вимірювання числа фотонів у імпульсі. У цьому випадку Єва змушена буде відводити фотон тільки у невеликої частини БФІ, а інші пропускати, не одержуючи ніякої інформації. Для захисту від атаки поділу числа фотонів можна використовувати вдосконалені протоколи КРК – протокол SARG04 та протоколи зі станами приманки (decoy states protocols) [1].

Атака поділу пучка фотонів (*photon beam splitting attack – PBS attack*). Процеси вимірювання числа фотонів в імпульсі та відведення одного фотона (якщо в імпульсі їх два або більше), що використовуються в PNS-атаці, дозволені квантовою механікою, але їх виконання знаходиться

поки що на межі можливостей сучасних технологій. Тому в ряді досліджень була запропонована більш проста та достатньо легко здійснювана з сучасними технологіями атака, що отримала назву атаки поділу пучка фотонів. Єва контролює друге вихідне плече світлодільника й одержує повне знання бітів просіяного ключа (через відстрочене вимірювання), якщо БФІ розділений таким чином, що Боб та Єва обоє одержують принаймні один фотон сигналу. Так, у роботі було запропоновано використовувати для такої атаки метод адаптивної абсорбції, що дозволяє вилучити точно один фотон з моди. Потужність атаки, що отримала назву *умовної атаки поділу числа фотонів*, наближається до потужності PNS-атаки. Один з методів захисту від PBS-атаки, як і від PNS-атаки, – це контролювання Бобом усієї статистики одержуваних сигналів, але для цього необхідно виконувати неруйнуюче вимірювання числа фотонів в імпульсі, що є дуже складним з технологічної точки зору. Тому, більш практичним на теперішній час є використання в системах КРК, замість протоколу BB84, удосконалених протоколів – SARG04 або протоколів зі станами приманки.

Атака заміни існуючого квантового каналу на кращий. Удосконалення PNS- та PBS-атак можливо таким способом: Єва таємно замінює квантовий канал зі втратами між Алісою та Бобом на ідеальний канал без втрат (або на канал зі значно меншими втратами) [16-18]. У такому випадку Єва зможе блокувати певну частину ОФІ, видаючи таки втрати за природні – тобто Боб отримає приблизно таку ж кількість пустих імпульсів, як до заміни каналу. Неважко помітити, що для початкового каналу з великими втратами Єва матиме можливість отримати майже весь ключ і залишиться непоміченою. Крім того, якщо рівень втрат у початковому каналі дуже значний, то Єва при заміні його на значно кращий зможе зберегти не лише очікувану Бобом частку пустих імпульсів, а й усю статистику числа фотонів у імпульсі [16]. Відзначимо, що атаку заміни існуючого квантового каналу на кращий практично дуже важко здійснити. У будь-якому випадку для захисту від такого типу атаки Аліса та Боб мають використовувати квантовий канал обмеженої довжини так, щоб його коефіцієнт передачі залишався достатньо високим [18].

Деякі інші атаки з використанням витоку інформації побічними каналами. У роботі [17] розглянута атака, за якої Єва вимірює просторові, спектральні або часові характеристики імпульсів, що передаються бездротовим оптичним каналом. Виконані в цій роботі експерименти з протоколом BB84 показують, що найбільшу інформацію про передані біти ключа – $6{,}6\times10^{-3}$ біт/імпульс – Єва може отримати при вимірюванні спектральних характеристик. Але ця величина є достатньо малою і, таким чином, цю атаку не можна вважати потужною. Інша атака, пов'язана з часовою незбалансованістю детектора, розглянута у праці [16] (*timing channel attack*). Дана атака, на відміну від попередніх, дозволяє Єві отримати значну частину секретного ключа. Технічні методи захисту від цієї атаки також запропоновані у [16].

Взагалі, теоретичні аспекти безпеки КК є на теперішній час дуже активною областю досліджень, але значно менше досліджень поки присвячено ретельному дослідженню практичних систем. Однак останнім часом спостерігається зростаючий інтерес до аналізу атак з використанням витоку інформації побічними каналами, що є результатом фізичної реалізації принципів КК в практичних системах.

Криптоаналітичні атаки на ПШД КСЗІ

У основі всіх практично існуючих на сьогодні КСЗІ лежить КРК (за протоколами BB84 та SARG04), а також шифрування класичними симетричними алгоритмами шифрування (АШ), наприклад AES. Виходячи з цього, було б логічно проаналізувати існуючі криптоаналітичні атаки, за допомогою яких Єва може нанести шкоду ПШД КСЗІ (атаки на АШ). Відповідно до принципу Керкгофа (Kerckhoffs' principle) безпека АШ має забезпечуватися і визначатися ключем шифрування, а сам АШ має бути відкритим та доступним. Зважаючи на це, можна зробити припущення, що Єві відомо повний обсяг необхідної інформації про АШ, який використовують Аліса з Бобом. У такому випадку Єва може реалізувати наступні типи атак: атака на основі тільки шифротексту (ШТ); на основі відкритого тексту (ВТ); на основі підібраного ВТ; на основі адаптивно підібраного ВТ; використанням підібраного ШТ; на основі підібраного ключа; методом повного перебору всіх можливих ключів; на основі апаратних помилок, кореляційна атака, бандитська криптоаналітична атака тощо. *Атака на основі тільки ШТ* (*cipher text attack*) полягає у тому, що Єва володіє ШТ ($N_1, N_2,\ldots, N_i$) декількох ВТ

(P_1, P_2,…, P_i), зашифрованих одним АШ. Єва розкриває якомога більшу кількість ШТ або ключів шифрування з метою розкриття інших ШТ, зашифрованих тим самим ключем (k). Тобто, маючи $N_1=E_k(P_1)$, $N_2=E_k(P_2)$,…, $N_i=E_k(P_i)$ можна визначити (P_1, P_2,…, P_i) та k або алгоритм відновлення P_{i+1} із $N_{i+1}=E_k(P_{i+1})$. *Атака на основі ВТ* (*plaintext attack*) реалізується таким чином, що Єва, володіючи ШТ (N_1, N_2,…, N_i) і їх ВТ (P_1, P_2,…, P_i), розкриває k з метою подальшого розшифрування інших ШТ, зашифрованих тим же ключем (ключами). Іншими словами, маючи P_1, $N_1=E_k(P_1)$, P_2, $N_2=E_k(P_2)$,…, P_i, $N_i=E_k(P_i)$, можна визначити k або алгоритм відновлення P_{i+1} із $N_{i+1}=N_k(P_{i+1})$. *Атака на основі підібраного ВТ* передбачає наявність у Єви шифрованих (N_1, N_2,…, N_i) і ВТ (P_1, P_2,…, P_i) декількох повідомлень, а також можливість підібрати ВТ для шифрування. Це надає більше можливостей, ніж розкриття на основі ВТ, оскільки Єва здійснює вибір блоків ВТ, що підлягають шифруванню і це може дати більше інформації про k. Таким чином, Єва отримує ключ чи АШ, що дозволяє розкрити нові повідомлення, зашифровані тим же ключем, тобто, маючи, P_1, $N_1=E_k(P_1)$, P_2, $N_2=E_k(P_2)$,…, P_i, $N_i=E_k(P_i)$ та можливість вибрати (P_1, P_2,…, P_i), Єва визначає k або алгоритм знаходження P_{i+1} із $N_{i+1}=E_k(P_{i+1})$. *Атака на основі адаптивно підібраного ВТ* передбачає можливість Єви вибирати ВТ (P_1, P_2,…, P_i), що підлягає шифруванню, а також уточнювати наступний вибір на базі раніше отриманих результатів шифрування. При розкритті з використанням підібраного ВТ Єва бере для шифрування лише один великий блок ВТ, а при адаптивному вибирається менший блок, і потім наступний, використовуючи результати першого вибору і т.д. *Атака з використанням підібраного ШТ* полягає у тому, що Єва для розкриття може вибирати різні ШТ (N_1, N_2,…, N_i) і має доступ до розшифрованих ВТ. Наприклад, маючи "чорний ящик", що реалізує автоматичне розшифрування, необхідно одержати ключ. Іншими словами, маючи $N_1P_1=D_k(N_1)$, $N_2P_2=D_k(N_2)$,…, $N_iP_i=D_k(N_i)$, Єва визначає k. Така атака зазвичай застосовується до систем з відкритим ключем, але іноді буває ефективною і для симетричних АШ. Часто в літературі атаку на основі підібраного ВТ і атаку з використанням підібраного ШТ разом називають *атакою на основі підібраного тексту*. *Атака на основі підібраного ключа* реалізується таким чином, що Єва має деяку інформацію про зв'язок між різними ключами. Даний тип криптоаналітичних атак часто буває дуже практичним і відрізняється від всіх раніше розглянутих. Єва вибирає зв’язок між парою невідомих ключів, за допомогою яких зашифровані дані. У варіанті з відомим ВТ є відкритий і шифрований двома ключами текст, а у варіанті з підібраним – Єва вибирає ВТ для шифрування двома ключами. *Атака методом повного перебору всіх можливих ключів* передбачає використання Євою відомого ШТ і реалізується шляхом тотального перебору усіх можливих ключів з одночасною перевіркою змістовності отриманого ВТ. Для реалізації такої атаки Єві необхідно застосувати надпотужні обчислювальні ресурси (зважаючи на довжину ключів у сучасних стійких АШ), через це іноді така атака носить назву *силової* (*лобової*) *атаки* (*brute force attack*). Останнім часом, зважаючи на стрімкий розвиток обчислювальних мереж, ефективність використання даного типу атак значно зросла, тобто Єва може об’єднати свої зусилля з іншими зловмисниками шляхом розпаралелювання певних операцій. *Атака на основі апаратних помилок* реалізується шляхом очікування або цілеспрямованої генерації Євою апаратних помилок в регістрах даних пристрою шифрування (системи, модуля). Завдяки такій атаці, Єва може з певною ймовірністю отримати фрагмент ключа шифрування, а з використанням додаткового програмного забезпечення розмір цього фрагменту може бути суттєво збільшений. Іноді даний тип атак називають *атаками аналізом збоїв*. Крім того, виділяють цілий клас *атак за допомогою побічних каналів* (*side-channel analysis attack*), тобто таких атак, за допомогою яких, на відміну від розглянутих вище, Єва намагається отримати інформацію про ключ чи ВТ не на основі теоретичного опису криптографічного АШ, а на основі даних, отриманих в результаті спостереження за фізичним процесом роботи пристрою шифрування. До даного класу атак відносять атаки *по часу, по енергоспоживанню, по електромагнітному випромінюванню, по світловому випромінюванню, акустичні атаки. Кореляційна атака (correlation attack)* основана на виявленні Євою статистичної залежності між елементами вхідної (P_1, P_2,…, P_i) і вихідної (N_1, N_2,…, N_i) послідовностей шифратора. На рис. 1 зображено перелік *підкласів кореляційних атак*. *Бандитська криптоаналітична атака* полягає у тому, що Єва загрожує, використовує тортури чи шантажує Алісу й Боба поки не отримає ключ шифрування. Досить вагомим і поширеним явищем є використання Євою хабарництва – *атака з "купленим ключем"* (*key purchase attack*).

Варто також відмітити, що коли реалізуються атаки, які використовують "людський чинник", то виявляються безсилими і найстійкіші криптографічні шифри, і навіть КСЗІ з безумовною стійкістю.

Висновки

Запропонована в даній статті розширена класифікація атак на КСЗІ враховує як атаки на підсистеми КРК та КПБЗ, так і атаки на класичні ПШД, що використовуються в якості модулів у гібридних системах захисту. Такі гібридні системи, що складаються з підсистеми КРК та звичайного шифрувального модуля, який використовує симетричні АШ (наприклад AES), пропонуються на теперішній час декількома компаніями [1, 2]. Дана класифікація атак дозволить чітко визначити напрямки подальших досліджень щодо розробки методів та побудови ефективних систем ЗІ, а також створити концептуальні аспекти квантової моделі попередження атак та формалізувати можливості превентивних систем для підвищення ефективності їх вибору і формуванні вимог при їх проектуванні та розробці.

Список літературних джерел

1. Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika, 2010, Vol. 14, No. 2, p. 58–69.

2. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко , Є.В. Василіу , С.О. Гнатюк // Захист інформації. – №1, 2010. – С. 77–89.

3. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). – М.: Постмаркет, 2002. – С. 33–73.

4. Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – V. 74, issue 1. – P. 145–195.

5. Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, А.Г. Корченко, Е.В. Пацира, С.А. Гнатюк // Проблеми інформатизації та управління: Зб. наук. праць. – К. : НАУ, 2009. – Вип. 4 (28). – С. 131–140.

6. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля – № 4 (146) – Ч. 1, 2010. – С. 184–193.

7. Розова Я.С. Классификация атак на каналы квантового распределения ключей / Я.С. Розова // Сборник трудов конференции молодых ученых, Выпуск 6. Инф. техн. – СПб: СПбГУ ИТМО, 2009. – С. 167–172.

8. Скобелев В.Г. Анализ атак на квантовый протокол передачи ключа / В.Г. Скобелев // Прикладная дискретная математика – № 2 (2), 2008. – С. 62–66.

9. Василиу Е.В. Стойкость квантовых протоколов распределения ключей типа "приготовление-измерение" / Е.В. Василиу // Georgian Electronic Scientific Journal: Computer Science and Telecommunications. – 2007, No. 2 (13), p. 50–62.

10. Молотков С.Н. О коллективной атаке на ключ в квантовой криптографии на двух неортог. состояниях / С.Н. Молотков // Письма в ЖЭТФ. – 2004. – Т. 80, вып.8. – С. 639–644.

11. Василиу Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василиу // Информатика: ОИПИ НАН Беларуси. – 2009, № 1 (21) – С. 117–128.

12. Hwang W. Eavesdropper's optimal information in variations of Bennett-Brassard 1984 quantum key distribution in the coherent attacks / W. Hwang, D. Ahn, S. Hwang // Physics Letters A. – 2001. – V. 279, issue 3–4. – P. 133–138.

13. Cai Q.-Y. The "ping-pong" protocol can be attacked without eavesdropping / Q.-Y. Cai // Physical Review Letters. – 2003. – Vol. 91, issue 10. – 109801.

14. Deng F.-G. Robustness of two-way quantum communication protocols against Trojan horse attack / F.-G. Deng, P. Zhou, X.-H. Li et al // [Електронний ресурс]. – Режим доступу: http://arxiv.org/abs/quant-ph/0508168.

15. Li X.-H. Improving the security of secure direct communication based on the secret transmitting order of particles / X.-H. Li, F.-G. Deng, H.-Y. Zhou // Physical Review A. – 2006. – V. 74, issue 5. – 054302.

16. Lutkenhaus N. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack / N. Lutkenhaus, M. Jahma // NJP. – 2002. – V. 4. – P. 44.1–44.9.

17. Williamson M. Eavesdropping on practical quantum cryptography / M. Williamson,V. Vedral // Journal of Modern Optics. – 2003. – V. 50, issue 13. – P. 1989–2011.

18. Niederberger A. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography / A. Niederberger, V. Scarani, N. Gisin // Physical Review A. – 2005. – V. 71, issue 4. – 042316.