

УДК 003.26:004.056.55:621.39

І.Д. Горбенко (ХНУРЕ), Є.В. Іванченко (НАУ),  
С.В. Карпенко (НАУ), С.О. Гнатюк (НАУ)

## МЕТОДИ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ У СИСТЕМАХ КВАНТОВОЇ КРИПТОГРАФІЇ

У даній статті запропоновано розширену класифікацію методів перехоплення інформації в системах квантової криптографії та розроблено модель порушника у таких системах. Отримані результати дозволяють підвищити ефективність роботи систем квантової криптографії та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем захисту інформації з використанням квантових технологій.

Ключові слова: захист інформації, квантова криптографія, перехоплення інформації, квантовий канал, модель порушника.

**Вступ.** На даний момент з усіх існуючих квантових технологій захисту інформації (ЗІ), до яких відносяться квантовий розподіл ключів (КРК), квантовий прямий безпечний зв'язок (КПБЗ), квантове розділення секрету, квантовий потоковий шифр, квантовий цифровий підпис та квантова стеганографія лише системи КРК є реалізованими практично, як окремі модулі та компоненти, що інтегровані в існуючі інформаційно-комунікаційні системи (ІКС) [1-3]. Системи КРК мають теоретико-інформаційну стійкість [1-3], що забезпечується законами квантової фізики. Якщо розподілені за допомогою квантової системи ключі будуть використані для шифрування за алгоритмом одноразового блокнота (Вернама), а також для аутентифікації користувачів з теоретико-інформаційною стійкістю [4], то можна створити повністю безпечний класичний канал зв'язку між двома користувачами. Фундаментальні закони квантової механіки [2, 3] з одного боку забезпечують виявлення атак на системи квантової криптографії (СКК), а з іншого – допускають можливість реалізації різного роду специфічних атак на такі системи. Зважаючи на те, що у квантовому каналі неможливо відрізнити природні завади від тих, що створюються порушниками при спробі перехоплення (знімання) інформації, необхідно передбачити цей факт при проектуванні та розробці превентивних систем.

**Аналіз існуючих досліджень.** У роботі [5] проведено якісний аналіз атак у кіберпросторі, а праця [6] містить розширену класифікацію кібератак за ознаковим принципом. 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 роботах [2, 3, 9]. Але загальна класифікація атак на СКК та методів знімання інформації в квантовому каналі зв'язку на даний момент відсутня у науковій літературі. Таким чином, виникають труднощі при побудові моделі порушника у СКК та оцінці можливостей таких систем протидіяти порушникам.

**Метою** даної роботи є підвищення ефективності розробки систем квантової криптографії за рахунок аналізу можливих методів перехоплення інформації (МПІ) у квантовому каналі та побудови моделі порушника у квантових системах.

**Загальна класифікація методів перехоплення інформації у СКК за ступенем складності.** Найпростішим способом знімання інформації у звичайних оптичних телекомунікаційних мережах є розділення пучка фотонів. Однак у протоколах квантової криптографії передавання повинно відбуватися за допомогою одиночних фотонів, і в такому випадку порушник не може відвести частину сигналу. Тому, подібні МПІ не можуть бути застосовані у СКК в ідеальних умовах однофотонних сигналів (до того ж, такі джерела сигналів поки що не створені). На практиці наразі використовують слабкі когерентні

імпульси, випромінювані лазерними світлодіодами. Число фотонів в імпульсі визначається розподілом Пуассона, тобто частина переданих імпульсів містить два й більше фотони. Ймовірність зареєструвати в імпульсі більше одного фотона при передаванні їх каналом зі втратами визначається за формулою:

$$p_{n>1} = 1 - e^{-\eta\mu} (1 + \eta\mu), \quad (1)$$

де  $\mu$  – середнє число фотонів в імпульсі,  $\eta$  – коефіцієнт передачі каналу.

Таким чином, МПІ з розділенням пучка фотонів на цей час можливі й у квантовій криптографії. На рис.1 наведена загальна класифікація МПІ у СКК.

Розглянемо спочатку МПІ, які можуть бути використані зловмисником при умові, що легітимні користувачі реалізують квантовий протокол з **ідеальними однофотонними джерелами сигналів**. У цьому випадку МПІ за ступенем складності можна поділити на *когерентні* та *некогерентні*. При некогерентних МПІ зловмисник обробляє кожний фотон, що передається квантовим каналом, окремо [3, 9, 10]. У свою чергу, некогерентні МПІ бувають *непрозорими* та *напівпрозорими*. Непрозорі МПІ полягають у вимірюванні зловмисником безпосередньо квантового стану фотона і подальшій повторній посиленні нового фотона у стані, який отримано в результаті вимірювання. Оскільки зловмисник не пропускає квантові стани відправника, а генерує нові і відправляє їх приймаючій стороні, то даний клас МПІ називається непрозорим.

МПІ при використанні легітимними користувачами ідеальних однофотонних джерел				МПІ, зумовлені недосконалістю протоколів		МПІ, зумовлені недосконалістю обладнання				
Когерентні		Некогерентні		Атака типу "людина посередині"	Атака типу "відмова в обслуговуванні"	МПІ, пов'язані з часовою незбалансованістю детектора	МПІ, пов'язані з заміною існуючого квантового каналу на кращий	Розділення пучка фотонів	Розділення числа фотонів	Атаки типу "Троянський кінь"
Об'єднані	Коллективні	Непрозорі	Напівпрозорі							

Рис.1. Узагальнена класифікація МПІ у СКК

Напівпрозорі МПІ [3, 9] передбачають використання зловмисником допоміжних квантових систем (квантових проб – КП) для переплутування їх з носіями, які суб'єкт А (відправник) пересилає суб'єкту Б (отримувачу) квантовим каналом. Після переплутування, передавані та допоміжні стани знаходяться у загальному переплутаному стані, потім перші передаються суб'єктові Б, а другі зберігаються у квантовій пам'яті у зловмисника. Після закінчення відкритого обміну інформацією між суб'єктами А та Б на етапі просіювання ключа, зокрема об'явлення базисів, в яких суб'єкт Б вимірював фотони, зловмисник визначає послідовність базисів, яку необхідно використати для вимірювання станів його проб, щоб отримати якомога більше інформації про ключ. Стани фотонів, що посилає суб'єкт А, змінюються після переплутування з пробами зловмисника, проте рівень помилок при даній атаці значно нижчий, ніж при непрозорій. Варто відмітити, що для реалізації подібного МПІ зловмиснику необхідно мати квантову пам'ять великого об'єму для зберігання проб до об'явлення базисів суб'єктом Б, а також складне обладнання для переплутування своїх проб з фотонами суб'єкта А. Напівпрозорі МПІ є також одним з основних видів знімання інформації в протоколах КПБЗ. У роботі [11] проаналізована атака з використанням КП на

пінг-понг протокол КПБЗ з ГХЦ-триплетами [1, 2], а також обчислено повну ймовірність виявлення атаки зловмисника у залежності від кількості отриманої ним інформації для трьох варіантів пінг-понг протоколу. Аналогічний аналіз атаки на пінг-понг протокол з переплутаними парами кутритів виконано у праці [12]. Доведено, що інформаційна місткість та стійкість різних варіантів даного протоколу є обернено пропорційними величинами.

При когерентних МПІ [3, 9, 10, 13] зловмисник може будь-яким (унітарним) способом переплутати пробу будь-якого розміру з групою передаваних фотонів. Одним із підвидів даного класу МПІ є *колективна атака* [3, 9, 10]. Дана атака схожа з напівпрозорою в початковій стадії, тобто кожен фотон, що посилає суб'єкт А, індивідуально переплутується з окремою пробєю. Отже, зловмисник отримує проби в таких же станах, як і при напівпрозорій атаці. Але після закінчення відкритого обміну інформацією між легітимними користувачами, зловмисник виконує так зване узагальнене вимірювання відразу на всіх КП, як на єдиній квантовій системі. Найефективнішим МПІ в квантових криптосистемах є об'єднана атака [3, 9] – це окремий випадок когерентних МПІ, коли зловмисник використовує єдину КП (з гільбертового простору [2] станів більшої розмірності) для переплутування з усією послідовністю фотонів, що суб'єкт А передає суб'єктові Б. Але цей МПІ є також і найбільш складним з технічної точки зору. Підводячи підсумки, слід відзначити, що відповідно до сучасного рівня технологій квантової інформатики реалізація когерентних МПІ не є можливою (на відміну від некогерентних), так як на сьогодні не існує необхідних для цього квантової пам'яті великого об'єму та багатокубітного квантового комп'ютера.

**Методи перехоплення інформації, зумовлені недосконалістю протоколів.** Недосконалість протоколів є серйозним чинником для реалізації різноманітних МПІ та інших атак в СКК. Найвідомішим МПІ цього класу є *атака "людина посередині" (man-in-the-middle attack)*. Для реалізації цієї атаки зловмисник має повністю контролювати класичний канал зв'язку між легітимними користувачами, тобто мати можливість замінювати усі повідомлення, що передаються класичним каналом зв'язку. Таким чином зловмисник має можливість повністю зняти інформацію, якою обмінюються легітимні користувачі у квантовому каналі (наприклад, дізнатись всі біти ключа), і при цьому не бути виявленим легітимними користувачами. Слід зазначити, що усі існуючі протоколи КРК і КПБЗ є вразливими до даної атаки [1]. Захист від такої атаки є загальновідомим – аутентифікація повідомлень легітимних користувачів у класичному каналі.

*Атака "відмова в обслуговуванні" (denial of service attack)* не є МПІ, це є метод порушення зв'язку між легітимними користувачами. Уперше для оригінального пінг-понг протоколу КПБЗ така атака була розглянута в роботі [14]. Суть її полягає у тому, що зловмисник не переплутує свою пробу з кубітом на шляху від суб'єкта Б до суб'єкта А, а просто вимірює стан кубіта на зворотному шляху від суб'єкта А до суб'єкта Б (тобто після кодування інформації суб'єктом А) – тим самим порушуючи взаємну кореляцію кубітів у суб'єктів А та Б. У результаті зловмисник не отримує ніякої корисної інформації, проте зруйнує квантовий канал між легітимними користувачами. У випадку протоколу з ГХЦ-триплетами зловмисник 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 квантової криптографії.

**Методи перехоплення інформації, зумовлені недосконалістю обладнання.** У класичній криптографії МПІ, зумовлені недосконалістю обладнання, називають також *МПІ, що використовують витік інформації побічними каналами*. МПІ такого типу можливі також і в квантовій криптографії.

*Атаки типу "Троянський кінь"*. До атак даного типу уразливі так звані двосторонні (two-way) протоколи КРК та КПБЗ, тобто протоколи, в яких фотони пересилаються від суб'єкта Б до суб'єкта А та назад. Прикладом такого протоколу є вищезгаданий пінг-понг протокол КПБЗ. Вперше атака типу "Троянський кінь" була запропонована в [3]. Зловмисник посилає світлові імпульси у квантовий канал, що з'єднує апаратуру легітимних користувачів, а 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 легітимні користувачі повинні залишити "двері відкритими" для своїх фотонів. Але вони могли б виявити додаткові фотони зломисника, так як при такій атаці відбувається збільшення енергії імпульсів. Тому зломисник повинен використовувати світло іншої довжини хвилі, ніж використовують легітимні користувачі, а саме такої довжини хвилі, до якої їх датчики є нечутливими [3]. Інший спосіб для зломисника приховати атаку полягає в тому, що він перехоплює сигнал, переданий від суб'єкта Б до суб'єкта А, і потім вставляє додатковий фотон у сигнал з часом затримки, коротшим ніж часове вікно датчика [3, 15]. Таким чином, суб'єкт А не може виявити цей додатковий фотон, оскільки він не спричинює спрацювання його датчика. Після кодувальної операції, яку виконує суб'єкт А, зломисник перехоплює сигнал знову й відокремлює додатковий фотон. Він може одержати повну інформацію про кодувальну операцію суб'єкта А, виконавши відповідне вимірювання. Такий варіант атаки отримав назву *"Троянського коня з затримкою фотона"* [15].

Для протидії атаці "Троянський кінь" з використанням фотонів інших довжин хвиль, ніж використовують легітимні користувачі, вони повинні встановити фільтр сигналів з іншими довжинами хвиль на вході свого обладнання [3, 15, 16]. На практиці легітимні користувачі повинні експлуатувати фільтр довжини хвилі для фільтрування фонового світла, особливо коли у якості квантового каналу використовується вільний простір (бездротовий оптичний канал). Таким чином, для легітимних користувачів немає проблеми запобігти такій атаці [3]. Для атаки "Троянського коня з затримкою фотона" суб'єкт А повинен використовувати світлодіодник 50/50 [15], щоб розділити кожний сигнал на дві частини й провести вимірювання 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 СКК не може гарантуватися тільки принципами квантової механіки, але обов'язково покладається також на технічні засоби [3].

До МПП, пов'язаних з недосконалістю обладнання відносяться також *атака розділення числа фотонів (photon number splitting attack – PNS attack)* та *атака розділення пучка фотонів (photon beam splitting attack – PBS attack)*.

Як зазначено вище, однофотонні джерела сигналів поки не створені й на практиці використовують слабкі когерентні імпульси, в яких можуть міститися два та більше фотонів. Таким чином, на існуючому на ринку СКК [1, 17-19], які використовують протокол BB84, стає можливим атака поділу числа фотонів [2, 20-22]. Для проведення такої атаки для кожного імпульсу, що посилається суб'єктом А, зломисник повинен виконати квантове неруйнівне 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 [20]. Якщо зломисник виявляє в імпульсі більше одного фотона, то він відводить один, дозволяючи іншим безперешкодно пройти до суб'єкта Б. Потім зломисник виконує переплутування перехопленого фотона зі своєї пробою і очікує, коли після завершення передавання легітимні сторони оголосять використані базиси. Виконуючи потім вимірювання стану проби, зломисник одержує точне значення переданого біта, не вносячи при цьому ніяких помилок у просіяний ключ, тобто його атака залишається невиявленою. Якщо ж імпульс несе один фотон, то стратегії зломисника можуть бути різними. Наприклад, він може просто пропускати всі однофотонні імпульси (ОФІ), що дозволить йому залишитися невиявленим. Однак, при малому середньому числі фотонів в імпульсі (на практиці обладнання налаштовують так, щоб це число було порядку 0,1) кількість багатифотонних імпульсів (БФІ) буде невеликою, і це не дозволить зломиснику одержати будь-яку суттєву інформацію про ключ. Інша стратегія полягає у тому, що зломисник виконує некогерентну

атаку на ОФІ. У цьому випадку, зрозуміло, він вносить помилки в просіяний ключ, кількість яких буде залежати як від типу атаки, так і від частки ОФІ при передачі ключа.

Ще одна стратегія для зломисника полягає у блокуванні частини ОФІ – у результаті суб'єкт Б одержує порожній імпульс, тобто його датчик не реєструє фотон. Таким блокуванням частки ОФІ зломисник збільшує частку БФІ, що дозволяє йому збільшити інформацію про ключ при тому ж рівні внесених у просіяний ключ помилок. Оскільки чутливість сучасних датчиків, які використовуються в комерційних СКК, невелика, і вони реєструють в середньому лише 20–30% одиночних фотонів, а крім цього також відбуваються втрати фотонів у каналі, то зломисник теоретично може таким чином приховати свою атаку. Але суб'єкт Б, знаючи ймовірність одержати порожній імпульс при наявному обладнанні, може виявити значне перевищення кількості порожніх імпульсів над очікуваним. Відзначимо, що суб'єкт Б 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 зломисник змушений буде відводити фотон тільки у невеликій частині БФІ, а інші пропускати, не одержуючи ніякої інформації. Для захисту від атаки розділення числа фотонів можна використовувати вдосконалені протоколи КРК – протокол SARG04 та протоколи зі станами приманки (decoy states protocols) [1, 23].

*Атака розділення пучка фотонів (PBS attack).* Процедури вимірювання числа фотонів у 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 розділення пучка фотонів [24, 25]. Зломисник контролює друге вихідне плече світлодільника й одержує повне знання бітів просіяного ключа (через відстрочене вимірювання), якщо БФІ розділений таким чином, що легітимні користувачі обоє одержують принаймні один фотон сигналу. Так, у роботі [24] було запропоновано використовувати для такої атаки метод адаптивної абсорбції, що дозволяє вилучити точно один фотон з моди. Потужність атаки, що отримала назву *умовної атаки розділення числа фотонів*, наближається до потужності PNS-атаки [24]. Один з методів захисту від PBS-атаки, як і від PNS-атаки, – це контролювання суб'єктом Б усієї статистики одержуваних сигналів [24, 25], але для цього необхідно виконувати неруйнуюче вимірювання числа фотонів у імпульсі, що є дуже складним з технологічної точки зору. Тому, більш практичним на теперішній час є використання у СКК, 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: зломисник таємно замінює квантовий канал зі втратами між легітимними користувачами на ідеальний канал без втрат (або на канал зі значно меншими втратами) [20-22, 24, 25]. У такому випадку зломисник зможе блокувати певну частину ОФІ, видаючи такі втрати за природні – тобто суб'єкт Б отримає приблизно таку ж кількість пустих імпульсів, як до заміни каналу. Неважко помітити, що для початкового каналу з великими втратами зломисник матиме можливість отримати майже весь ключ і залишитись непоміченим. Крім того, якщо рівень втрат у початковому каналі дуже значний, то зломисник при заміні його на значно кращий зможе зберегти не лише очікувану суб'єктом Б частку пустих імпульсів, а й усю статистику числа фотонів у імпульсі [20]. Відзначимо, що атаку заміни існуючого квантового каналу на кращий практично дуже важко здійснити. У будь-якому випадку для захисту від такого типу атаки легітимні користувачі повинні використовувати квантовий канал обмеженої довжини так, щоб його коефіцієнт передачі залишався достатньо високим [22].

**Деякі методи перехоплення інформації з використанням витоку інформації побічними каналами.** У роботі [26] розглянута атака, за якої зломисник 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 –  $6,6 \times 10^{-3}$  біт/імпульс – злоумисник 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 (*timing channel attack*), розглянута у праці [27]. Дана атака, на відміну від попередніх, дозволяє злоумиснику отримати значну частину секретного ключа. Технічні методи захисту від цієї атаки також запропоновані у [27].

Взагалі, теоретичні аспекти безпеки квантової криптографії є на теперішній час дуже активною галуззю досліджень, але значно менше досліджень поки присвячено ретельному дослідженню практичних СКК. Однак, останнім часом спостерігається зростаючий інтерес до аналізу МПІ з використанням побічних каналів, що є результатом фізичної реалізації методів квантової криптографії в практичних СКК.

**Модель порушника у СКК.** Як зазначалося раніше, метою злоумисника є *несанкціонований доступ (НСД)* [5] до ресурсів ІКС (у даному випадку СКК) з різною ціллю. Виключенням є випадок, коли злоумисник ненавмисно реалізує НСД – у такому випадку він є *порушником*, але не злоумисником [28]. Особливу небезпеку можуть нести порушники, які знаходяться під впливом кримінальних угруповань, бізнесових структур, політичних організацій, спецслужб тощо. Припустимим характером дій таких порушників може бути прагнення отримання певних даних для їх подальшого використання, модифікації чи знищення з метою досягнення певних умов для себе чи структур, під впливом яких вони знаходяться. Варто також відзначити, що порушник може бути як внутрішнім (з числа співробітників чи легітимних користувачів), так і зовнішнім (перебуває за межами контрольованої зони ІКС або проникнув до неї несанкціонованим шляхом).

*Кваліфікація порушника* – сукупність певних знань і вмінь порушника, які він використовує для реалізації несанкціонованого доступу до ІКС, зокрема СКК. Можна відзначити кілька типів кваліфікації порушників, що дозволять успішно реалізувати загрози системам квантової криптографії:

- порушник володіє інформацією щодо функціональних особливостей СКК взагалі, уміє користуватися штатними засобами;
- порушник має високий рівень знань і досвід роботи в технічному обслуговуванні аналогічних СКК;
- порушник володіє високим рівнем знань в галузі обчислювальної техніки (зокрема, криптографії, теорії алгоритмів та паралельних обчислень тощо) і програмування на мовах розробки програмного забезпечення (ПЗ) для СКК або їх аналогів;
- порушник досконало володіє знаннями квантової фізики, квантової оптики тощо, а також навиками роботи з обладнанням, що використовується у СКК [2];
- порушник має доступ до глобальних обчислювальних мереж, суперкомп'ютера чи квантового комп'ютера, за допомогою якого може реалізувати, наприклад, силову атаку, використовуючи відомі квантові алгоритми Шора, Гровера тощо [29].

*Можливості порушника* щодо впливу на СКК можна представити у вигляді такої ієрархічної класифікації:

- 1) порушник має можливість запуску певного обмеженого набору ПЗ, що реалізує певні функції з обробки класичної та квантової інформації;
- 2) порушник може створювати власне ПЗ та модифікувати існуюче, що дозволить створити нові функції обробки класичної і квантової інформації та подальшого одержання частини необхідної порушнику інформації;
- 3) порушник має змогу управляти функціонуванням СКК, тобто безпосередньо впливати на ПЗ, склад та конфігурацію технічного забезпечення ІКС;

4) порушник має весь обсяг можливостей легітимних користувачів – може розробляти та впроваджувати в експлуатацію технічні засоби ІКС, а також інтегрувати власні технічні засоби з метою подальшого отримання корисної йому інформації.

Підкреслимо, що теоретичний аналіз стійкості протоколів квантової криптографії, як правило, проводиться виходячи з того, що порушник має технічні можливості, обмежені тільки законами квантової механіки, а не поточним рівнем розвитку технологій.

*Цілі порушника* у СКК – це створення нових та підвищення ефективності існуючих методів аналізу стійкості класичних криптографічних засобів та засобів КРК і КПБЗ. Підґрунтям цілеспрямованої реалізації порушником НСД до ресурсів ІКС є найчастіше корисливі мотиви, хоча іноді буває бажання самовираження чи нанесення моральної шкоди легітимним користувачам.

Порушник може використовувати сукупність *релевантних знань, умінь та навиків*, для прикладу:

– *досконале знання математичного апарату* дозволить йому створити нові методи криптоаналізу відповідно до рівня криптографічного захисту;

– *знання мов програмування* дозволить порушнику реалізувати створені методи криптоаналізу, а також модифікувати існуюче ПЗ легітимних користувачів, в тому числі ПЗ СКК;

– *знання квантової фізики* дасть змогу порушнику підібрати відповідний МПІ та отримати корисну інформацію;

– *знання методів соціального інжинірингу* може дозволити порушнику без ґрунтовних знань математики, фізики та програмування обійти системи захисту як класичні, так і квантові.

За *характером дій* порушників можна класифікувати таким чином:

1) *випадковий порушник*, що помилково, ненавмисне і несвідомо порушив політику безпеки ІКС;

2) *терплячий порушник* безпеки, що порушив політику безпеки певного сегменту чи усієї ІКС свідомо, навмисно, але без рішучих дій, маскуючись, підбираючи атрибути доступу легітимних користувачів з метою подолання засобів управління доступом тощо;

3) *рішучий зловмисник*, що має на меті порушити одну із властивостей інформаційних ресурсів ІКС. Він прагне подолати усі існуючі засоби обмеження доступу і отримати можливість безпосереднього доступу до ресурсів ІКС з метою втручання у роботу системи, модифікації класичної чи квантової інформації, отримання необхідних даних тощо;

4) *віддалений порушник*, що аналізує технічні канали витоку інформації, впливає віддалено за допомогою спеціальних засобів на локальні та розподілені мережі ІКС, включаючи квантовий та класичний канали СКК.

Для більш детальної побудови моделі порушника, виходячи із конкретної СКК, рекомендується також класифікувати порушників за такими ознаками [30]:

– за підготовкою до подолання системи фізичного захисту ІКС;

– за характером поведінки;

– за інформованістю про об'єкт атаки (СКК);

– за використовуваними методами та засобами;

– за місцем реалізації атаки тощо.

**Висновки.** Запропонована у даній статті класифікація методів перехоплення інформації у СКК дозволяє чітко визначити напрямки подальших досліджень щодо розробки методів та побудови 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. Розроблена модель порушника в квантових системах ЗІ дозволяє визначити сукупність заходів різного характеру для організації комплексної системи ЗІ в ІКС.



### Література:

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. 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.
3. Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // *Reviews of Modern Physics*. – 2002. – V. 74, issue 1. – P. 145–195.
4. Wegman M. N. New hash functions and their use in authentication and set equality / M. N. Wegman, J. L. Carter // *Journal of Computer and System Science*. – 1981. – V. 22. – P. 265–279.
5. Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, А.Г. Корченко, Е.В. Пацера, 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. Пацера, 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. Василю Е.В. Стойкость квантовых протоколов распределения ключей типа "приготовление-измерение" / Е.В. Василю // *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. Василю Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василю // *Информатика: ОИПИ НАН Беларуси*. – 2009, № 1 (21) – С. 117–128.
12. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // *Quantum Information Processing*. – 2011. – V. 10, num. 2. – P. 189–202.
13. 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.
14. Cai Q.-Y. The "ping-pong" protocol can be attacked without eavesdropping / Q.-Y. Cai // *Physical Review Letters*. – 2003. – Vol. 91, issue 10. – 109801.
15. Deng F.-G. Robustness of two-way quantum communication protocols against Trojan horse attack / F.-G. Deng, P. Zhou, X.-H. Li et al // [Электронный ресурс]. – Режим доступа: <http://arxiv.org/abs/quant-ph/0508168>.
16. 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.
17. Toshiba Quantum Key Distribution System. Toshiba Research Europe Ltd. – [Электронный ресурс]. – Режим доступа: <<http://www.toshiba-europe.com/research/crl/QIG/quantumkeyserver.html>>.
18. MAGIQ QPN 8505 Security Gateway (QPN – 8505). – [Электронный ресурс]. – Режим доступа: <[http://www.magiqtech.com/MagiQ/Products\\_files/8505\\_Data\\_Sheet.pdf](http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf)>.
19. Cerberis. – [Электронный ресурс]. – Режим доступа: <<http://idquantique.com/products/cerberis.htm>>.
20. 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.
21. Williamson M. Eavesdropping on practical quantum cryptography / M. Williamson, V. Vedral // *Journal of Modern Optics*. – 2003. – V. 50, issue 13. – P. 1989–2011.
22. 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.
23. Scarani V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al // *Review of Modern Physics*. – 2009. – V. 81, issue 3. – P. 1301–1350.
24. Calsamiglia J. Conditional beam splitting attack on quantum key distribution / J. Calsamiglia, S.M. Barnett, N. Lutkenhaus // *Physical Review A*. – 2001. – V. 65, issue 1. – 012312.
25. Felix S. Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses / S. Felix, N. Gisin, A. Stefanov, H. Zbinden // *Journal of Modern Optics*. – V. 48, issue 13. – P. 2009–2021.
26. Nauerth S. Information leakage via side channels in freespace BB84 quantum cryptography / S. Nauerth, M. Furst, et al // *New Journal of Physics*. – 2009. – V. 11, issue 6. – 065001.



27. Lamas-Linares A. Breaking a quantum key distribution system through a timing side channel /A. Lamas-Linares, C. Kurtsiefer // Optics Express. – 2007. – V. 15, issue 15. – P. 9388–9393.

28. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник. – К. : Видавництво DIRECTLINE, 2009. – 714 с.

29. Корченко О.Г. Квантові технології конфіденційного зв'язку / О.Г. Корченко, С.О. Гнатюк, В.М. Кінзерявий // Защита информации: Сб. науч. трудов. – К. : НАУ, 2010. – Вып. 1. – С. 179–184.

30. Дровникова И.Г. Модель нарушителя в системе безопасности / И.Г. Дровникова, Т.А. Буцынская // Системы безопасности. – 2008, № 5. – С. 144–147.

Надійшла: 11.05.2011 р.

Рецензент: д.т.н., проф. Хорошко В.О.