УДК 003.26:004.056.55:621.39

С.О. Гнатюк, асистент, С.О. Демченко, здобувач, В.М. Кінзерявий, асистент
(Національний авіаційний університет, Україна)

БАЗОВІ ОЗНАКИ КЛАСИФІКАЦІЇ КІБЕРАТАК НА КВАНТОВІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

У даній роботі запропоновані базові ознаки класифікації кібератак на квантові системи розподілу ключів та прямого безпечного зв'язку. Отримані результати дозволяють формалізувати напрямки подальших досліджень щодо розробки більш ефективних квантових систем захисту інформації.

Вступ. На даний момент з усіх існуючих квантових технологій захисту інформації (ЗІ) [1] лише системи на основі квантового розподілу ключів (КРК) є реалізованими практично, як окремі модулі та компоненти, інтегровані в існуючі інформаційно-комунікаційні системи (ІКС). Фундаментальні закони квантової механіки [1, 6] 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 [2] проведено якісний аналіз атак у кіберпросторі (cyber space), а праця [6] містить розширену класифікацію кібератак (cyber attack) за ознаковим принципом. Крім того, у роботі [3] наведена класифікація атак на канали КРК: виділено два класи таких атак – це атаки на кубіти та атаки, що використовують неідеальність компонентів системи. Класифікація атак на КРК за критерієм складності необхідного для проведення атаки обладнання наведена у [4, 6]. Така узагальнена базова 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)). *Метою* даної роботи є розробка класифікації кібератак на квантові системи захисту інформації за ознаковим принципом. Реалізація поставленої мети дозволить формалізувати напрямки подальших досліджень щодо розробки та побудови ефективних систем ЗІ на основі квантових технологій.

На рис. 1 наведена узагальнена класифікація кібератак на КСЗІ.

Класифікація атак за ступенем складності. На основі [1, 3, 4] можна ввести наступне визначення – *атаками у КСЗІ* називаються заходи, які застосовуються для підриву безпеки даних систем чи реалізації загроз базовим характеристикам безпеки систем квантової криптографії (КК) шляхом використання їх уразливостей. При використанні легітимними користувачами *ідеальних однофотонних джерел*, атаки в системах КК можна умовно поділити на *когерентні* та *некогерентні*. У свою чергу, некогерентні (індивідуальні) атаки [4, 6] бувають *непрозорими* (*opaque attacks*) та *напівпрозорими* (*semi-translucent attacks*). Непрозорі атаки (їх також називають *атаками "перехоплення – повторної посилки кубітів", intercept-resend attack* [6]) 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 генерує нові квантові стани і відправляє їх приймаючій стороні (Бобові), то даний клас атак називається непрозорим. Напівпрозорі атаки [4, 6] 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

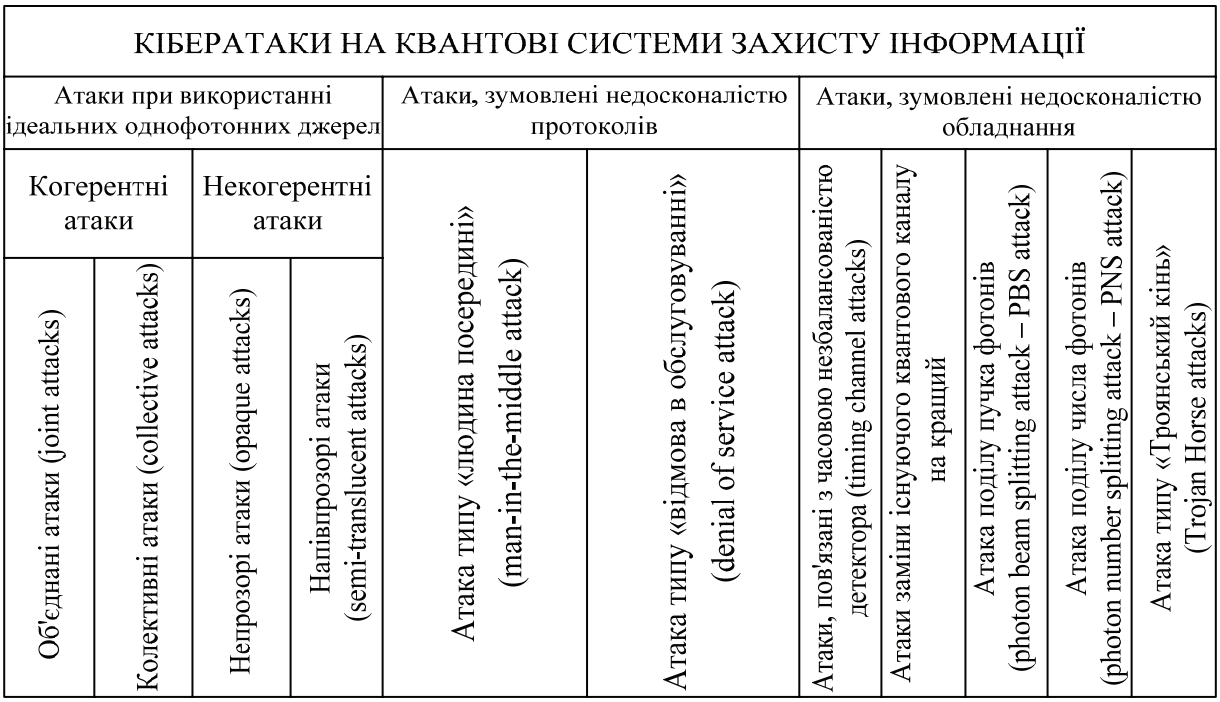

Рис.1. Узагальнена класифікація кібератак на КСЗІ

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.

При когерентних атаках [4, 6] 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*). 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*) – 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.

Атаки, зумовлені недосконалістю протоколів. 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.

Що стосується атаки "відмова в обслуговуванні", то 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 [6]. Відзначимо, що до атаки "відмова в обслуговуванні" також вразливі практично всі протоколи КК.

Атаки, зумовлені недосконалістю обладнання

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. Єва посилає світлові імпульси у квантовий канал, що з’єднує апаратуру Аліси та Боба, і потім аналізує відбите світло. Таким спосо-

бом 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. 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. 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"*. 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). Для атаки "троянського коня з затримкою фотона" Аліса повинна використовувати світлодільник 50/50, щоб розділити кожний сигнал на дві частини й провести вимірювання їх станів у двох вимірювальних базисах [6].

Атака поділу числа фотонів (*photon number splitting attack – PNS attack*). На практиці в системах КРК використовують слабкі когерентні імпульси, випромінювані лазерними світлодіодами [6]. Число фотонів в імпульсі визначається розподілом Пуассона, тобто частина переданих імпульсів містить два й більше фотони. 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 [5]. 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 подібної атаки необхідно використовувати 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 знаходяться поки що на межі можливостей сучасних технологій. Тому в ряді досліджень була запропонована 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. 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 удосконалених протоколів – SARG04 або протоколів зі станами приманки [6].

Атака заміни існуючого квантового каналу на кращий. У випадку таємної заміни квантового каналу зі втратами між Алісою та Бобом на ідеальний канал без втрат (або на канал зі значно меншими втратами) [5], 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. 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 [6].

Атаки з використанням витоку інформації побічними каналами. У роботі [6] розглянута атака, пов'язана з часовою незбалансованістю детектора (*timing channel attack*). Дана атака, на відміну від попередніх, дозволяє Єві отримати значну частину секретного ключа. Технічні методи захисту від цієї атаки на даний час також запропоновані.

Взагалі, теоретичні аспекти безпеки КК є на теперішній час дуже активною областю досліджень, і останнім часом спостерігається зростаючий інтерес до аналізу атак з використанням витоку інформації побічними каналами, що є результатом фізичної реалізації принципів КК в практичних системах.

Висновки. Запропонована в даній роботі базова класифікація кібератак на КСЗІ враховує як атаки на підсистеми КРК так і на підсистеми КПБЗ. Дана класифікація атак дозволяє 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 формування вимог при їх проектуванні та розробці.

Список використаної літератури:

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. 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.

3. 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.

4. 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.

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

6. Атаки в квантових системах захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. – 2010. – №2. – С.109–115.