Тобто застосування НШС сигналів з метою забезпечення високочастотного впливу гіпотетично може мати суттєві переваги перед застосуванням вузькосмугових сигналів і становити загрозу конфіденційності ІзОД.

Висновки

Останнім часом суттєвого розвитку набули системи зв'язку і радіолокації на основі НШС сигналів, що зумовило їх значне розповсюдження у повсякденній діяльності. Властивості НШС сигналів суттєво відрізняються від властивостей, притаманних вузькосмуговим сигналам і не завжди пояснюються класичною теорією зв'язку.

З огляду на зазначене вище пропонується і планується провести достатньо глибокі науково обґрунтовані теоретичні і експериментальні дослідження щодо загрози формування технічного каналу витоку інформації в умовах високочастотного впливу НШС сигналами на тракти основних технічних засобів.

Список літератури

1. Имнореев И.Я. Сверхширокополосные радары: новые возможности, необычные проблемы, системные особенности // Вестник МГТУ, №4, 1998, - С. 25-56.

2. Скосырев В.Н., Особенности и свойства сверхкороткоимпульсной локации. Конспекты лекций. – ССРС, Россия, Муром, Июль 2003, - С. 67-91.

3. Fontana R.J., Recent System Applications of Short-Pulse Ultra-Wideband (UWB) Technology // IEEE Transactions on microwave theory and techniques, vol. 52, № 9, September 2004.

4. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок : затверджено наказом Державної служби України з питань технічного захисту інформації від 09 червня 1995 р. № 25.

5. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с.

6. Каторин Ю.Ф. Антишпионские штучки. Энциклопедия промышленного шпионажа / Каторин Ю.Ф. – СПб. : Полигон, – 1999. – 564 с.

7. Ярочкин В.И. Предпринимательство и безопасность. Ч. 1. Несанкционированный доступ к источнику конфиденциальной информации / Ярочкин В.И. – М. : Экспрессное бюро, – 1994. – 64 с.

Надійшла 3.11.09

УДК 003.26:004.056.55:621.39 **Корченко О.Г., Васіліу Є.В., Гнатюк С.О.**

СУЧАСНІ КВАНТОВІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні першочерговим чинником, що впливає на складові національної безпеки, є ступінь захищеності інформаційного середовища. Питання інформаційної безпеки набуває актуальності як у процесі стрімкого розвитку комп'ютерних технологій, так і у контексті різкого збільшення злочинів та інших протиправних дій, спрямованих на порушення конфіденційності, цілісності та достовірності інформації. Основна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними із базових задач якої є: розподіл ключів шифрування, аутентифікація сторін, авторизація легітимних користувачів [1]. Розподіл ключів шифрування (криптографічних ключів) між законними користувачами в умовах суворої секретності є однією з найважливіших проблем криптографії, яка може бути вирішена за допомогою [2]:

- класичної криптографічної схеми з теоретико-інформаційної стійкістю (для її реалізації необхідний канал з перешкодами; ефективність схеми вкрай низька – 1-5%);

- класичної криптографічної схеми з відкритим ключем (схема Діфі-Хелмана, схема цифрового конверту; має обчислювальну стійкість);
- класичної симетричної криптографічної схеми з обчислювальною стійкістю (потребує наявності у абонентів попередньо встановленого ключа, тобто може розглядатися тільки як схема для збільшення довжини ключа, а не для його розподілення);
- квантового розподілу ключів (забезпечує теоретико-інформаційну стійкість, але потребує наявності у абонентів попередньо встановленого ключа для аутентифікації класичного каналу, тобто теж може розглядатися як схема для збільшення довжини ключа);
- методу довірених кур'єрів (висока вартість, велика залежність від людського фактору).

В останні роки значний інтерес викликає квантова криптографія [2, 3, 6, 8-10, 12, 23, 24], вагоме місце в якій займає квантовий розподіл ключів [3-5, 7-22, 25-31]. Переважна більшість теоретичних та практичних досліджень у галузі квантової криптографії присвячена саме розробці та вдосконаленню квантових протоколів розподілу ключів (КПРК), які поряд з іншими квантовими криптографічними протоколами становлять сукупність методів захисту інформації (ЗІ) на основі квантових технологій. Кількість останніх з часом невпинно зростає, проте в науковій літературі відсутня чітка класифікація таких методів та засобів, що ускладнює пошук і не дає змоги у повній мірі оцінити рівень існуючих досягнень для їх подальшого ефективного використання. *Метою даної роботи* є систематизація та класифікація сучасних квантових технологій захисту інформації, якісний аналіз переваг та недоліків, перспектив та труднощів їх практичного впровадження.

До складу квантових технологій захисту інформації (рис.1) входять: квантовий розподіл ключів [3-5, 7-22, 25-31], квантовий прямий безпечний зв'язок [4, 32-39], квантове розділення секрету [40-45], квантовий потоковий шифр [46-53], квантовий цифровий підпис [54-57] та квантова стеганографія [58-60].

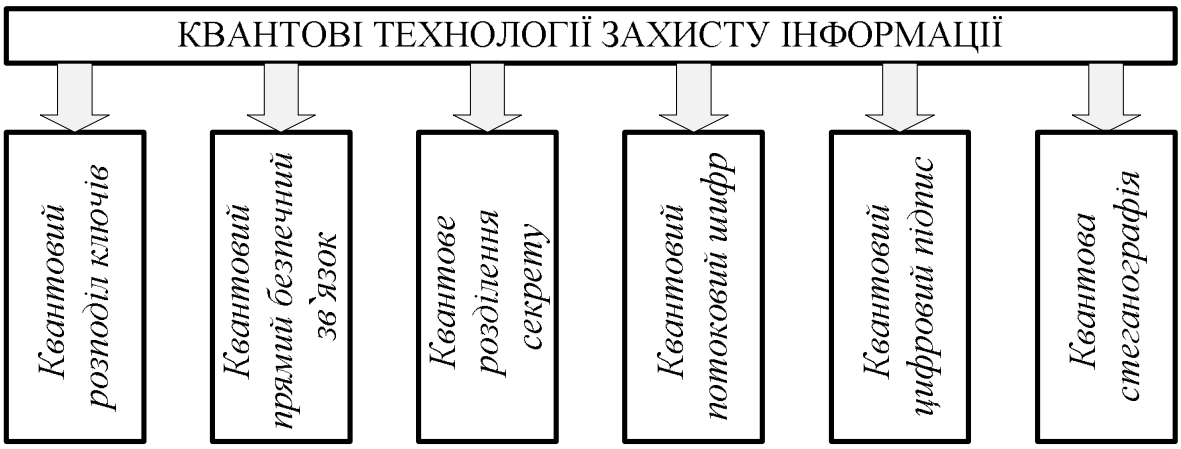

Рис.1. Квантові технології захисту інформації

Квантовий розподіл ключів включає в себе наступні протоколи (рис. 2):
- протоколи з використанням одиничних поляризованих фотонів [2, 7-20];
- протоколи з використанням фазового кодування [11, 19];
- протоколи з використанням переплутаних станів [21, 22, 25, 26];
- протоколи зі станами «приманки» [27-31].

У 1984 році Ч. Беннет з компанії IBM та Ж. Брассар з Монреальського університету запропонували перший протокол квантової криптографії [2, 3, 7], що мав стати альтернативним і нетрадиційним рішенням проблеми розподілу ключів шифрування. Даний протокол отримав назву *BB84* [8-10], він відноситься до протоколів квантового розподілу ключів *з використанням одиничних поляризованих фотонів*. Основними задачами КПРК є

генерація та розподіл ключів шифрування між двома абонентами, що з'єднані квантовим та класичним каналами зв'язку [11]. У протоколах з одиничними поляризованими фотонами використовуються 4 поляризовані стани фотонів (0º, 45º, 90º, 135º), які передаються квантовим каналом зв'язку [10]. Пошук та виправлення помилок виконується з використанням відкритого класичного каналу, який не повинен бути конфіденційним, тільки аутентифікованим. Для виявлення факту дій зловмисника використовується процедура контролю помилок, а для забезпечення безумовної стійкості використовується класична процедура підсилення секретності (privacy amplification) [12].

Ефективність протоколу BB84 з кубітами в ідеальних умовах дорівнює 50%. Під ефективністю розуміють відношення кількості фотонів, що використовуються для генерації ключа, до загальної кількості переданих фотонів. Крім того, в роботі [13] запропоновано узагальнення протоколу BB84 на багаторівневі квантові системи (так званий протокол BB84 з кудитами). Цей протокол має значно більшу інформаційну місткість та стійкість до некогерентних атак, але його складніше реалізувати з технічної точки зору [14]. Вихідними даними КПРК є ключова послідовність, яка може бути використана для подальшого шифрування даних. До вищезгаданого типу протоколів (див. рис. 2) крім BB84 відносяться також протокол з шістьома станами [15], протокол 4+2 [16], протокол Гольденберга-Вайдмана [17] та протокол Коаші-Імото [18].

Рис.2. Класифікація квантових протоколів розподілу ключів

Протокол *з шістьома станами* [15] передбачає використання чотирьох станів, аналогічних протоколу BB84, і додатково вводяться ще два можливих напрямки поляризації – правоциркулярний та лівоциркулярний. Такі зміни з одного боку зменшують кількість інформації, що може бути отримана зловмисником, а з іншого боку ефективність протоколу також зменшується (до 33%). Також запропоновано узагальнення протоколу з шістьома станами на багаторівневі квантові системи. Даний протокол має дещо більшу інформаційну місткість та значно більшу стійкість до атаки «перехоплення – повторної посилки» кудитів. Стійкість протоколу до загальної некогерентної атаки практично така ж, як і протоколу BB84 з кудитами [13, 14].

Протокол *4+2* [16] є перехідним між BB84 та B92. У ньому використовуються чотири квантових стани для кодування «0» та «1» у двох базисах. Стани в кожному базисі вибираються неортогональними, крім того, стани в різних базисах також мають бути попарно неортогональними. Для протоколу 4+2 характерна менша кількість помилок відносно протоколу BB84 для кубітів і менша кількість корисної інформації, що може

отримати зловмисник, але одночасно відбувається й зменшення відносної ефективності протоколу.

У протоколі *Гольденберга-Вайдмана* [17] кодування «0» та «1» виконується за допомогою двох ортогональних станів. Кожен з цих двох станів є суперпозицією двох локалізованих нормалізованих хвильових пакетів. Для захисту проти атаки «перехоплення – повторної посилки» використовується випадковий час відправлення пакетів. Модифікований варіант протоколу Гольденберга-Вайдмана – це протокол *Коаші-Імото* [18], удосконалений тим, що замість випадкового часу відправлення пакетів використовується асиметризація інтерферометра, тобто світло розбивається у нерівних пропорціях між довгим і коротким плечами інтерферометра.

Наступний тип КПРК – протоколи квантового розподілу ключів *з використанням фазового кодування* [11]. Одним з представників даного типу протоколів є протокол B92 [19] з використанням потужних імпульсів [11]. Але в протоколі B92 зловмисник може одержати більше інформації про ключ для заданого рівня створюваних їм помилок, чим у протоколі BB84, тобто стійкість протоколу B92 нижче стійкості протоколу BB84 [20]. Ефективність протоколу B92 становить 25%.

Протокол *Екерта* (він же *E91*) [11, 21, 22], відноситься до КПРК *з використанням переплутаних станів*, властивості яких детально описані в роботах [6, 23, 24]. Під час передавання інформації за протоколом E91 перехоплення одного із фотонів пари не дає зловмиснику ніякої корисної інформації. Крім того, запропоновано узагальнення схеми Екерта на тривимірні [25], та багатовимірні [26] квантові системи, що значно збільшує інформаційну місткість протоколу.

Протоколи *зі станами «приманки»* (decoy states protocols) є удосконаленим варіантом протоколу BB84, у якому відправник, шляхом заміни підмножини імпульсів, вводить так звані приманки [27]. Як показують практичні експерименти [28, 29], даному типу протоколів характерний більш високий рівень безпеки, ніж у BB84. Крім того, такі протоколи відзначаються стійкістю проти атаки розділення кількості фотонів (photon number splitting attack) [30, 31]. До явних переваг протоколів зі станами «приманки» також можна віднести і збільшення довжини каналу за рахунок лінійної залежності від втрат у каналі. Проте, без попередньої аутентифікації користувачів на таких протоколах не можливо побудувати завершене повноцінне рішення проблеми розподілення криптографічних ключів.

Таким чином, проаналізувавши перший та найбільш масштабний тип методів ЗІ на основі квантових технологій – КПРК, можна підбити певні підсумки і виділити переваги та недоліки квантових протоколів розподілу ключів. До переваг можна віднести наступне:

1. Протоколи КПРК дозволяють завжди виявити атаку пасивного перехоплення (eavesdropping), так як підключення зловмисника вносить до квантового каналу значно більший рівень помилок порівняно з природнім рівнем.

2. Безумовна (теоретико-інформаційна) безпека КПРК, що дозволяє використати абсолютно секретний ключ для подальшого шифрування відомими класичними симетричними алгоритмами – це відповідно збільшить рівень захищеності, який забезпечують суто класичні криптосистеми. Також можливий синтез КПРК з шифром Вернама (одноразовим блокнотом) [1], що в поєднані з безумовно стійкою схемою аутентифікації дасть абсолютно стійку систему обміну повідомленнями.

До недоліків квантових протоколів розподілу ключів відносяться:

1. Система, побудована тільки на КПРК, не може слугувати повноцінним завершеним рішенням (потрібні засоби для попередньої аутентифікації користувачів).

2. Обмеження довжини квантового каналу, тобто неможливість підсилення без втрати квантових властивостей.

3. Швидкість передачі інформації квантовим каналом суттєво зменшується зі збільшенням довжини каналу і на відстанях порядку 100 км дорівнює декільком бітам за секунду.

4. Проблеми реєстрації фотонів – ефект «темнового шуму».

5. Залежність каналу від зовнішнього впливу.

6. Деполяризація фотонів у квантовому каналі.

7. Складність технічної реалізації протоколів з багатовимірними квантовими системами.

8. Висока ринкова ціна комерційних рішень, що робить їх недоступним для більшості вітчизняних користувачів.

Квантовий прямий безпечний зв'язок. Наступним методом захисту інформації на основі квантових технологій є використання квантових протоколів прямого безпечного зв’язку (КППБЗ) [4, 32-39]. Характерною особливістю даного методу є відсутність криптографічних перетворень, відповідно відсутня і проблема розподілу ключів шифрування. Протоколи КППБЗ можна поділити на чотири типи (рис. 3): пінг-понг протокол (різні його варіанти) [33-35, 37], протоколи з передаванням переплутаних кубітів блоками [32, 36], протоколи з одиничними кубітами та протоколи з групами переплутаних кудитів [36].

Більшість запропонованих до теперішнього часу квантових протоколів прямого безпечного зв’язку потребують передачі кубітів блоками. Це дозволяє виявити прослуховування квантового каналу до початку передачі самого повідомлення й таким способом гарантувати безпеку передачі – якщо прослуховування виявлене до передачі повідомлення, то легітимні сторони переривають сеанс і ніяка інформація не витікає до зловмисника. Але для зберігання таких блоків кубітів необхідна квантова пам'ять великого об'єму. Технологія квантової пам'яті активно розробляється, але поки ще далека від масового застосування в стандартному телекомунікаційному встаткуванні. Тому з погляду технічної реалізації перевагу мають протоколи, у яких передача здійснюється одиничними кубітами або невеликими їхніми групами (за один цикл протоколу). Таких протоколів запропоновано небагато, і вони мають тільки асимптотичну безпеку, тобто атака буде виявлена з високою ймовірністю, але до цього зловмисник зможе одержати деяку частину повідомлення. Отже, виникає проблема підсилення безпеки таких протоколів, тобто створення таких методів попередньої обробки передаваної інформації, які зроблять перехоплену зловмисником інформацію даремною для нього.

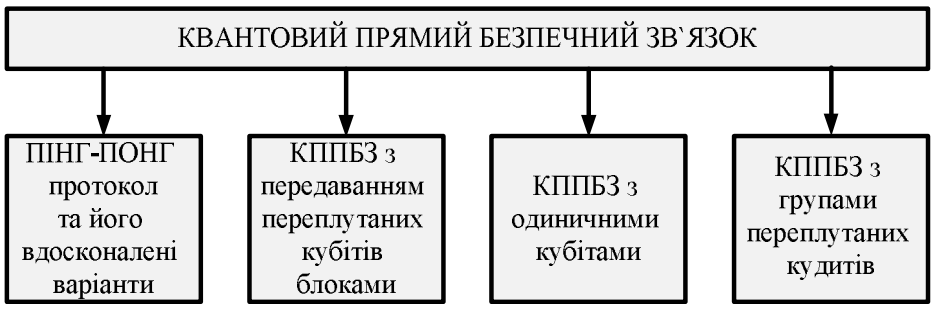

Рис. 3. Протоколи квантового прямого безпечного зв’язку

Одним із КППБЗ, який не потребує квантової пам'яті великого об'єму, є *пінг-понг протокол* [3, 33]. У своєму початковому варіанті протокол використовує переплутані пари кубітів (ЕПР-пари) і дозволяє передати один біт класичної інформації за один цикл протоколу. Використання квантового надщільного кодування дозволяє передати два біти за цикл протоколу [34]. Подальше збільшення інформаційної місткості можливе шляхом використання замість переплутаних пар кубітів їх трійок, четвірок і т.д., що перебувають у переплутаних станах Грінбергера-Хорна-Цайлінгера (ГХЦ) [35]. Інформаційна місткість

пінг-понг протоколу із ГХЦ-станами дорівнює n бітів на цикл, де n – кількість кубітів у використовуваних ГХЦ-станах. Інший шлях підвищення інформаційної місткості пінг-понг протоколу – це використання переплутаних станів багаторівневих квантових систем (кудитів). Так, відповідний протокол з використанням станів Бела пари трирівневих систем (кутритів) та квантового надщільного кодування для кутритів був розроблений у роботах [36, 37].

Загалом крім ЕПР-пар та ГХЦ-триплетів квантовий прямий безпечний зв'язок передбачає використання груп з чотирьох та більше переплутаних кубітів у ГХЦ-станах або кластерних станах. Також для даного типу протоколів характерне використання квантового надщільного кодування, унітарних перетворень станів кубітів, наявність класичного аутентифікованого каналу зв’язку.

До переваг КППБЗ слід віднести: відсутність необхідності у розподіленні секретних ключів, можливість обміну інформацією більш ніж між двома користувачами і центром, можливість виявлення атаки зловмисника, а також забезпечення високого рівня захищеності (аж до теоретико-інформаційної безпеки) для протоколів з передаванням кубітів блоками. Що стосується недоліків, то перш за все слід відзначити ймовірність замаскованої атаки на пінг-понг протокол у квантовому каналі з шумом. У роботі [38] запропоновано атаку на оригінальний варіант пінг-понг протоколу, що використовує два додаткових фотони, які переплутуються з передаваним фотоном застосуванням певних квантових гейтів. Ця атака не може бути виявлена в режимі контролю підслуховування (стандартному для оригінального протоколу), але створює 50%-ні втрати в каналі, що може бути легко виявлено легітимними користувачами, якщо природний рівень шуму в каналі невеликий. У роботі [39] атака була вдосконалена таким чином, що додаткові втрати в каналі не створюються, однак обидва варіанти цієї атаки створюють додатковий передаваний фотон, що може бути зареєстрований передавачем та приймачем і свідчить про операції зловмисника. Також ці атаки створюють додатковий рівень помилок в 25% у режимі передачі повідомлення, що також можуть виявити легітимні користувачі. Ще один спосіб виявити таку атаку – застосування двох вимірювальних базисів в режимі контролю підслуховування замість одного базису, як в оригінальному пінг-понг протоколі. При використанні двох базисів імовірність виявлення атаки становить 25% [39].

Також до недоліків КППБЗ слід віднести складність практичної реалізації (аналогічно КПРК з кудитами), невисоку швидкість передачі кубітів, потребу в квантовій пам'яті великого об’єму для всіх учасників сеансу зв'язку (для протоколів з передаванням кубітів блоками) та асимптотичну безпеку пінг-понг протоколу (яка однак може бути підсилена методами класичної криптографії). Крім того, КППБЗ, як і КПРК, є вразливими до атаки «людина посередині», хоча дана атака й може бути нейтралізована шляхом аутентифікації всіх передаваних у класичному каналі повідомлень.

Квантове розділення секрету. Переважна частина квантових протоколів розділення секрету (КПРС) використовує властивості *переплутаних квантових станів* [6, 23, 24]. Перший КПРС був запропонований Hillery, Buzek та Berthiaume у 1998 році [40, 41], який, аналогічно деяким протоколам квантового безпечного зв'язку, використовує ГХЦ-триплети (четвірки) кубітів. Цей протокол дозволяє відправнику розділити своє повідомлення між двома (трьома) абонентами таким чином, що вони зможуть його прочитати, тільки діючи спільно.

У роботі [42] запропоновано *напів-квантовий* КПРС з використанням ГХЦ-триплетів (четвірок) кубітів. У цьому протоколі сторони, що приймають розділене повідомлення, мають доступ до квантового каналу, але обмежені деяким набором операцій та називаються «класичними», в тому сенсі, що вони не мають можливості готувати переплутані стани, виконувати будь-які квантові операції та вимірювання. Дані сторони можуть вимірювати кубіти у «класичному» $\{|0\rangle,|1\rangle\}$ базисі, впорядковувати їх за допомогою затримок

вимірювань, приготувати кубіти у «класичному» базисі, а також відправляти або повертати кубіти без збурення їх станів. Сторона, що розділяє своє повідомлення, може виконувати будь-які квантові операції. Цей протокол має перевагу над іншими КПРС з економічної точки зору – обладнання у приймальних сторін буде дешевше, оскільки їм не потрібно дороге обладнання для створення багатокубітних переплутаних станів та вимірювань, наприклад, в ГХЦ-базисі. До напів-квантових КПРС відносяться дві групи протоколів – це напів-квантові КПРС, що ґрунтуються на рендомізації, та КПРС, що ґрунтуються на «вимірюванні – повторній відправці» кубітів.

У роботі [43] представлено КПРС *з використанням одиничних фотонів*, що готуються у двох взаємно незміщених базисах і посилаються блоками. Цей протокол, аналогічно протоколу Hillery-Buzek-Berthiaume, дозволяє відправнику розділити своє повідомлення між двома абонентами (або більшою кількістю абонентів). Удосконалення стійкості запропонованого у праці [43] протоколу проти зловмисних дій одного з легітимних користувачів було виконано в роботі [44]. Аналогічний протокол для багатостороннього розділення секрету запропонований у роботі [45].

Усі КПРС є захищеними як проти зовнішнього зловмисника, так і проти нечесних дій учасників протоколу. На відміну від класичних схем розділення секрету, квантові та напів-квантові схеми дозволяють виявити підслуховування та не потребують шифрування повідомлень. Найзначнішим недоліком більшості КПРС є потреба у наявності великої квантової пам'яті в усіх сторін, що поки знаходиться за межами можливостей сучасних технологій.

Квантовий потоковий шифр (КПШ) передбачає шифрування даних подібно до класичних потокових шифрів, але із застосуванням квантового шумового ефекту [46] і може використовуватись в оптичних комунікаційних мережах. КПШ базується на протоколі *Yuen 2000 (Y-00)* [46-53], який ще називають *αη-схема* [47]. Вихідними даними передавача у даній схемі є послідовність когерентних станів, що переносить інформацію про дані чи ключ. Теоретико-інформаційна стійкість протоколу Y-00 забезпечується рендомізацією, що базується на квантовому шумі, а також на додаткових математичних (обчислювальних) схемах [48, 50]. У роботах [50, 51] експериментальним шляхом продемонстровано високу швидкість шифрування даних по протоколу Y-00, а у праці [52] показана ідеальна кореляційна захищеність, тобто стійкість до швидких кореляційних атак. Ще однією перевагою КПШ є більша захищеність порівняно із звичайними потоковими шифрами завдяки квантовому шумовому ефекту і неможливості клонування квантових станів [3, 46, 51, 53]. Що стосується недоліків КПШ, то варто відмітити, перш за все, складність практичної реалізації системи [52].

Квантовий цифровий підпис (КЦП) може бути реалізований на наступних протоколах:

- *протоколи з одиничними фотонами* [54];
- *протоколи з переплутаними станами* (автентичний КЦП, оснований на квантових кореляціях ГХЦ) [55].

Квантовий цифровий підпис базується на фундаментальних принципах квантової фізики [6, 8-10, 12, 23, 24, 53] і полягає у використанні односторонньої функції [56], яка, на відміну від класичної, є більш захищеною з теоретико-інформаційної точки зору (тобто її захищеність не залежить від потужності обладнання зловмисника – забезпечується теоретико-інформаційна безпека).

Квантова одностороння функція визначається наступними властивостями квантових систем [56]:

- на відміну від класичних бітів, кубіти можуть існувати у суперпозиціях «0» та «1»;

- згідно теореми Холево [6, 57] кількість класичної інформації, яку можна отримати із квантового стану, є обмеженою. Обчислення і перевірка функції не є складними але зворотне обчислення є неможливим.

У системах, що використовують КЦП, ідентифікація користувачів та цілісність інформації забезпечується аналогічно класичному цифровому підпису [1, 56]. До основних переваг КЦП варто віднести теоретико-інформаційну захищеність та спрощену систему розподілу ключів. Головним же недоліком є можливість генерування обмеженої кількості копій відкритого ключа, крім того, на відміну від ідеальної класичної односторонньої функції, завжди є витік певної кількості інформації про вхідні дані квантової необоротної функції [56].

Квантова стеганографія [58] аналогічно класичній має за мету приховання самого факту передачі інформації. Хоча на даний момент не відомо жодної практичної реалізації систем квантової стеганографії, проте у кількох працях [58, 59] пропонуються моделі систем, що використовують квантову стеганографію. Усі існуючі моделі систем квантової стеганографії використовують властивості *переплутаних станів*, так, наприклад, у роботі [60] для приховування факту передачі інформації використовуються модифіковані методи детекції переплутаних пар фотонів. Оскільки теоретичні дослідження у даній галузі ще не вийшли на рівень практичного застосування, тому важко говорити про переваги і недоліки систем квантової стеганографії, відповідно залишається відкритим питання про більшу практичну ефективність таких систем у порівнянні з системами, що використовують класичну стеганографію.

На рис. 4 представлена загальна схема класифікації квантових методів захисту інформації за їх призначенням, а також за використовуваними квантовими технологіями.

Сучасні засоби ЗІ на основі квантових технологій. Першим у світі комерційним рішенням квантової криптографії була система *QPN Security Gateway (QPN-8505)* [61], запропонована компанією MagiQ Technologies (США). Дана система є економічно вигідним рішенням ЗІ для урядових і фінансових організацій, пропонує захист VPN за допомогою квантового розподілу ключів (до ста 256 бітних ключів у секунду на відстань до 140 км) та інтегрованого шифрування. Система QPN-8505 використовує протоколи: BB84, 3DES [62], AES [63]. Варто відзначити, що система QPN Security Gateway для більшості потенційних клієнтів (зокрема у нашій державі) є недоступною через високу вартість (близько 50 тис. €).

Швейцарська компанія ID Quantique пропонує систему під назвою *Cerberis* [64], що являє собою сервер з автоматичним створенням і секретним обміном ключами через захищений оптоволоконний канал (FC-1G, FC-2G та FC-4G). Дана система може передавати криптографічні ключі на відстань до 50 км, її характерною особливістю являється 12 паралельних криптографічних обчислень, що значно підвищує швидкодію. Система Cerberis використовує для шифрування протокол AES (256 біт), а для квантового розподілення ключів – протоколи BB84 та SARG. Також нещодавно компанією Toshiba Research Europe Ltd (Великобританія) було представлено ще одну систему КРК під назвою *Quantum Key Server* [65]. Ця система відрізняється простотою своєї архітектури та забезпечує генерацію до ста 256 бітних ключів у секунду та їх односторонню передачу від передавача до приймача. До її складу входить інтегрований модуль автоматичного управління, що проводить неперервний моніторинг системи Quantum Key Server і регулює оптичні характеристики. Ще одна британська компанія QinetiQ представила першу у світі мережу, що використовує квантову криптографію – *Quantum Net (Qnet)* [66, 67]. Максимальна довжина ліній зв'язку даної мережі становить 120 км, та найголовнішим є те, що система Qnet – це перша квантово-криптографічна система, що використовує більше 2 серверів. Їх в даній системі аж 6 і всі вони є інтегрованими в Internet. Крім того, вчені провідних країн світу приймають активну участь у реалізації проектів, таких як SECOQC (Secure Communication based on Quantum Cryptography) [2] та EQCSPOT (European Quantum Cryptography and Single Photon

Technologies), інтенсивно ведуться теоретичні та практичні роботи по розробці засобів ЗІ на основі квантових технологій відомими науково-дослідними інститутами та центрами (Northwestern University, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research, Національна лабораторія в Лос-Аламосі) [68].

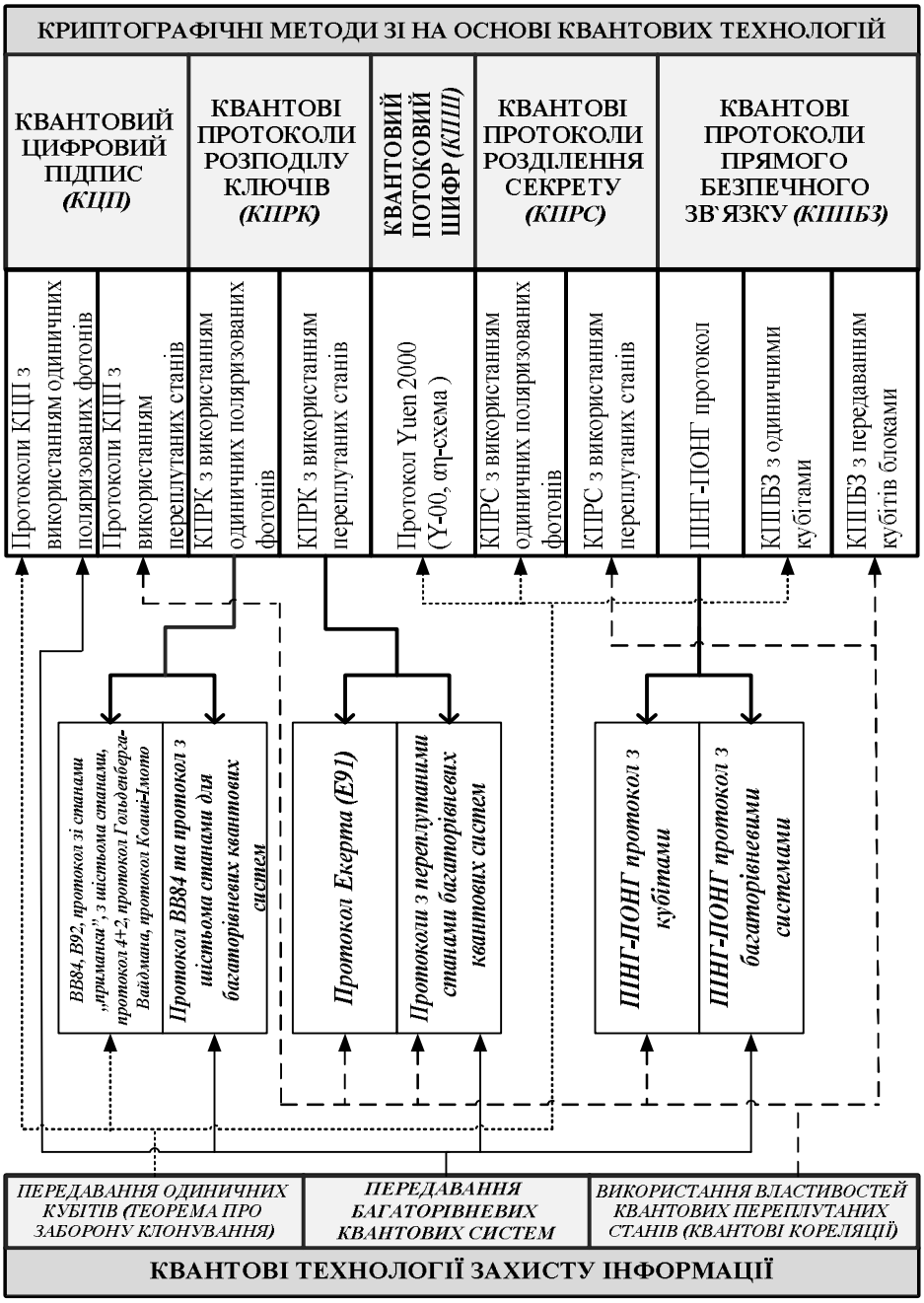

Рис.4. Класифікація квантових методів захисту інформації

Багато методів та засобів квантової криптографії є запатентованими [69-77] у різних країнах світу і мають перспективу бути реалізованими уже в найближчому майбутньому.

Висновки

У роботі виконано систематизацію та класифікацію сучасних квантових технологій захисту інформації. Дана характеристика основних напрямків квантової криптографії з точки зору використовуваних квантових технологій, проаналізовані переваги та недоліки

конкретних квантових протоколів. Показано, що найбільш розвиненим напрямком квантової криптографії на теперішній час є квантові протоколи розподілу ключів.

На теперішній час розроблені квантові криптографічні системи, призначені для розподілу секретних ключів між віддаленими легітимними користувачами. Частка використовуваних у цих системах технологій захищена патентами різних країн (переважно США). Такі системи квантового розподілу ключів можуть бути об'єднані з будь-якою іншою криптографічною схемою, яка забезпечує теоретико-інформаційну стійкість шифрування і при цьому вся схема також буде мати теоретико-інформаційну криптографічну стійкість. Взагалі, у багатьох випадках квантові протоколи розподілу ключів здатні забезпечити більш високий рівень безпеки систем захисту інформації, ніж відповідні класичні схеми.

Що стосується решти квантових технологій захисту інформації, то на практичному рівні вони поки що не вийшли за межі лабораторних експериментів. Але вже запропоновано велику кількість теоретичних схем, для яких доведено їх високу стійкість, аж до теоретико-інформаційної. Так, квантові протоколи прямого безпечного зв'язку, які взагалі не мають аналогів у класичній криптографії, знімають проблему розподілу секретних ключів, так як зовсім не використовують шифрування. Але один з класів таких протоколів – пінг-понг протокол та його вдосконалені варіанти, – забезпечує тільки асимптотичну безпеку (без використання додаткових методів підсилення його безпеки), а інший клас – протоколи з передаванням кубітів блоками – потребують наявності квантової пам'яті, яка поки що знаходиться за межами сучасних технологій.

Квантові протоколи розділення секрету теж мають перевагу над відповідними класичними протоколами, так як дозволяють виявити підслуховування у квантовому каналі та не потребують шифрування. Аналогічно, більш високий рівень безпеки, у порівнянні з відповідними класичними схемами, забезпечує квантовий потоковий шифр та квантовий цифровий підпис. Останній, завдяки використанню квантової односторонньої функції, має теоретико-інформаційну стійкість. Проте, практична реалізація цих квантових методів захисту інформації теж поки що зіштовхується з деякими технологічними складнощами.

Таким чином, квантові технології ЗІ бурхливо розвиваються в останні роки та поступово займають своє місце серед інших засобів захисту інформації, що обумовлено їх високим рівнем стійкості та властивостями, яких немає у класичних засобів ЗІ, наприклад, можливістю завжди виявити атаку пасивного перехвату. Але для практичного використання квантових технологій захисту інформації в існуючій інфраструктурі мереж передавання даних необхідно вирішити ще ряд завдань як теоретичного, так і особливо практичного характеру.

Список літератури

1. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

2. *SECOQC* White Paper on Quantum Key Distribution and Cryptography. – Preprint: http://www.arxiv.org/abs/quant-ph/0701168v1. – 2007. – 28 p.

3. *Гомонай О.В.* Лекції з квантової інформатики: Навчальний посібник. – Вінниця: О. Власюк, 2006. – С. 62–74.

4. *Василиу Е.В., Воробиенко П.П.* Проблемы развития и перспективы использования квантово-криптографических систем // Наук. праці ОНАЗ ім. О.С. Попова. – 2006, № 1. – С. 3–17.

5. *Bennett C.H., Bessette F., Brassard G. et al.* Experimental Quantum Cryptography // Journal of Cryptography. – 1992. – V. 5, № 1.– С. 3–28.

6. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 824 с.

7. *Bennett C. H., Brassard G.* Quantum cryptography: public key distribution and coin tossing // Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. – Bangalore, India. – 1984. – P. 175-179.

8. *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.

9. *Слепов Н.* Квантовая криптография: передача квантового ключа. Проблемы и решения // Электроника: НТБ. – 2006, №2. – С. 54–61.

10. *Румянцев К.Е., Голубчиков Д.М.* Квантовая криптография: принципы, протоколы, системы / Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. – 37 с.

11. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Review of Modern Physics. – 2002. – V. 74. – P. 145–195.

12. *Гиршов Е.* Доклад «Введение в квантовую криптографию» (основные понятия, протоколы, примеры, технологические аспекты) // <http://www.teormin.ifmo.ru/courses/intro/38.pdf>.

13. *Cerf N.J., Bourennane M., Karlsson A., Gisin N.* Security of quantum key distribution using d-level systems // Physical Review Letters. – 2002. – V. 88, №12. – 127902.

14. *Василиу Е.В., Мамедов Р.С.* Сравнительный анализ эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с передачей многомерных квантовых систем // Наукові праці ОНАЗ ім. О.С. Попова. – 2008, № 2. – С. 20–27.

15. *Bruss D.* Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters. – 1998. – V. 81, № 14. – P. 3018–3021.

16. *Huttner B., Imoto N., Gisin N., Mor T.* Quantum Cryptography with Coherent States // Physical Review A. – 1995. – V. 51, № 3. – P. 1863–1869.

17. *Goldenberg L., Vaidman L.* Quantum Cryptography Based On Orthogonal States // Physical Review Letters. – 1995. – V. 75, № 7. – P. 1239–1243.

18. *Koashi M., Imoto N.* Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps // Physical Review Letters. – 1997. – V. 79, № 12. – P. 2383–2386.

19. *Bennett C.H.* Quantum cryptography using any two non-orthogonal states // Physical Review Letters. – 1992. – V. 68, № 21. – P. 3121–3124.

20. *Fuchs C., Gisin N., Griffits R. B. et al*. Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy // Physical Review A. – 1997. – V. 56, № 2. P. 1163–1172.

21. *Ekert A.* Quantum cryptography based on Bell's theorem // Physical. Review Letters. – 1991. – V. 67, № 6. – 661–663.

22. *Inamori H., Rallan L., Vedral V*. Security of EPR-based quantum cryptography against incoherent symmetric attacks // Journal of Physics A. – 2001. – Vol. 34, № 35. – P. 6913 – 6918.

23. *Качаев И.А.* Квантовые вычисления. – Протвино, 2001. – 24 с. – (Препр. / Государственный научный центр РФ. Институт физики высоких энергий; 2001-12).

24. *Стин Э.* Квантовые вычисления. Перевод с английского И.Д. Пасынкова: НИЦ «Регулярная и хаотическая динамика», Москва – Ижевск, 2000. – 111 с.

25. *Kaszlikowski D. Oi D.K.L., Christandl M. et al* Quantum cryptography based on qutrit Bell inequalities // Physical Review A. – 2003. – V. 67, № 1. – 012310.

26. *Durt T., Kaszlikowski D., Chen J.-L., Kwek L.C.* Security of quantum key distributions with entangled qudits // Physical Review A. – 2004. – V. 69, №3. – 032313.

27. *Wang X.-B.* Comment on "Decoy State Quantum Key Distribution" // arXiv:quant-ph/0501143.

28. *Rosenberg D. et al.* Long-distance decoy-state quantum key distribution in optical fiber // Physical. Review Letters. – 2007. – V. 98, № 1. – 010503.

29. *Peng C.-Z., Zhang J., Yang D. et al.* Experimental long-distance decoy-state quantum key distribution based on polarization encoding // Physical Review Letters. – 2007. – V. 98, № 1. – 010505.

30. *Dusek M., Haderka O., Hendrych M.* Generalized beam-splitting attack in quantum cryptography with dim coherent states // Optics Communications. – 1999. – V. 169. – P. 103–108.

31. *Brassard G., Lutkenhaus N., Mor T., Sanders B. C.* Limitations on practical quantum cryptography // Physical Review Letters. – 2000. – V. 85, № 6. – P. 1330–1333 (2000).

32. *Chuan W., Fu Guo D., Gui Lu L.* Multi-step quantum secure direct communication using multi-particle Greenberg-Horne-Zeilinger state. – Optics Communications. – 2005. – V. 253. – P. 15–19.

33. *Bostrom K., Felbinger T.* Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

34. *Cai Q.-Y., Li B.-W.* Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – 054301.

35. *Василиу Е.В., Василиу Л.Н.* Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171–176.

36. *Wang Ch., Deng F.-G., Li Y.-S. et al.* Quantum secure direct communication with high dimension quantum superdense coding // Physical Review A. – 2005. – V. 71, № 4. – 044305.

37. *Василиу Е.В., Мамедов Р.С.* Анализ атаки пассивного перехвата на пинг – понг протокол с полностью перепутанными парами кутритов // Восточноевропейский журнал передовых технологий. – 2009, № 4/2 (40). – С. 4–11.

38. *Wojcik A.* Eavesdropping on the «Ping-Pong» Quantum Communication Protocol // Physical Review Letters. – 2003. – V. 90, № 15. – 157901.

39. *Zhang Zh.-J., Li Y., Man Zh.-X.* Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss // Physics Letters A. – 2005. – V. 341, № 5–6. – P. 385–389.

40. *Hillery M., Buzek V., Berthiaume A.* Quantum secret sharing // Physical Review A. – 1999. – V. 59, № 3. – P. 1829–1834.

41. *Qin S.-J., Gao F., Zhu F.-Ch.* Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol // Physical Review A. – 2007. – V. 76, № 6. – 062324.

42. *Li Q., Chan W. H., Long D-Y.* Semi-quantum secret sharing using entangled states // arXiv:quant-ph/0906.1866v3.

43. *Zhang Z. J., Li Y., Man Z. X.* Multiparty quantum secret sharing // Physical Review A. – 2005. – V. 71, №4. – 044301.

44. *Deng F. G., Li X. H., Zhou H. Y., Zhang Z. J.* Improving the security of multiparty quantum secret sharing against Trojan horse attack // Physical Review A. – 2005. V. 72, № 4. – 044302.

45. *Yan F.-L., Gao T., Li Yu.-Ch.* Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations // Chinese Physics Letters. – 2008. – V. 25, № 4. – P. 1187 – 1190.

46. *Hirota O., Sohma M., Fuse M., Kato K.* Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme // Physical Review A. – 2005 – V. 72, № 2. – 022335.

47. *Nair R., Yuen H. P.* On the Security of the Y-00 (AlphaEta) Direct Encryption Protocol // arXiv:quant-ph/0702093v2.

48. *Yuen H. P.* In Proceedings of QCMC'00, Capri, 2001, edited by P. Tombesi and O. Hirota Plenum Press, New York, 2001.

49. *Yuen H. P.* KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation // arXiv:quant-ph/0311061.

50. *Barbosa G.A., Corndorf E., Kumar P., Yuen H.P.* Secure Communication Using Mesoscopic Coherent States // Physical Review Letters. – 2003. – V. 90, № 22. – 227901.

51. *Corndorf E., Liang C., Kanter G.S. et al.* Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks // Physical Review A. – 2005. – V. 71, № 6. – 062326.

52. *Hirota O., Kurosawa K.* An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol // arXiv:quant-ph/0604036v1.

53. *Wooters W.K., Zurek W.H.* A single quantum cannot be cloned // Nature. – 1982. – V. 299. – P. 802.

54. *Wang J., Zhang Q., Tang C.* Quantum signature scheme with single photons // Optoelectronics Letters. – 2006. – V. 2, N. 3. P. 209–212.

55. *Xiao-Jun W., Yun L.* Authentic Digital Signature Based on Quantum Correlation // arXiv:quant-ph/0509129v2.

56. *Gottesman D., Chuang I.* Quantum digital signatures // arXiv:quant-ph/0105032v2.

57. *Holevo A. S.* Problems in the mathematical theory of quantum communication channels // Report of Mathematical Physics. – 1977. – V. 12, №2. – P. 273–278.

58. Quantum Computation and Information. From Theory to Experiment / Imai H., Hayashi M. (eds.). – Springer-Verlag: Berlin, Heidelberg, 2006. – P. 235.

59. *Curty M., Santos D. J.* Quantum steganography // In 2nd Bielefeld Workshop on Quantum Information and Complexity. – 2000. – Bielefeld, Germany. – P. 12.

60. *Pat.* № 7539308 USA, H04K 1/00 (20060101). Quantum steganography / Conti, Ralph, Kenneth et al – 21.05.2004.

61. *MagiQ.* Products. QPN Security Gateway. [Електронний ресурс]. — Режим доступу: http://www.magiqtech.com/MagiQ/Products.html.

62. *NIST.* "FIPS-46-3: Data Encryption Standard." Oct. 1999. [Електронний ресурс]. — Режим доступу: http://csrc.nist.gov/publications/fips.

63. *NIST.* "FIPS-197: Advanced Encryption Standard." Nov. 2001. [Електронний ресурс]. — Режим доступу: http://csrc.nist.gov/publications/fips.

64. *ID* Quantique. Cerberis. [Електронний ресурс]. — Режим доступу: http://www.idquantique.com/products/cerberis.htm.

65. *QKS.* Toshiba Research Europe Ltd., Cambridge Research Laboratory. [Електронний ресурс]. — Режим доступу: http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html.

66. *Elliot C., Pearson D., Troxel G.* Quantum Cryptography in Practice // arXiv:quant-ph/0307049.

67. *Hughes R., Nordholt J., Derkacs D., Peterson C.* Practical free-space quantum key distribution over 10 km in daylight and at night // New Journal of Physics. – 2002. –V. 4. – 43.

68. *Алексеев Д.А., Корнейко А.В.* Практическая реальность квантово-криптографических систем распределения ключей // Захист інформації. – 2007. – №1. – С.72–76.

69. *Пат.* № 43779 України, МПК H04L 9/08. Система передачі криптографічних ключів / Гнатюк С.О., Кінзерявий В.М., Корченко О.Г., Паціра Є.В. – №u200904239; заявл. 29.04.2009; опубл. 25.08.2009, Бюл. №16.

70. *Пат.* № 2302085 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. – № 200513476; 16.11.2005.

71. *Пат.* № 2325039 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. – № 2006119652; 06.06.2006.

72. *Pat.* № 7461323 USA, H03M 13/00 (20060101). Quantum key delivery method and communication device / Matsumoto, Wataru et al – 02.12.2008.

73. *Pat.* № 7266304 USA, H04B 10/00 (20060101), H04K 1/00 (20060101). System for secure optical transmission of binary code / Duraffourg, Laurent et al – 04.09.2007.

74. *Pat.* № 7178277 USA, H04K 1/00 (20060101). Quantum cryptography communication system and quantum cryptography key distributing method used in the same / Takeuchi, Takeshi et al – 20.02.2007.

75. *Pat.* № 6748081 USA, H04L 9/08 (20060101), C09K 19/02 (20060101), G02F 1/13 (20060101). Quantum cryptography system for a secure transmission of random keys using a polarization setting method / Dultz, Wolfgang et al – 08.06.2004.

76. *Pat.* № 6438234 USA, H04L 9/08 (20060101), H04K 001/00. Quantum cryptography device and method / Gisin, Zbinden et al – 20.08.2002.

77. *Pat.* № 6895092 USA, H04L 9/08 (20060101), G06F 017/00. Cryptographic key distribution method and apparatus thereof / Tomita, Akihisa et al – 17.05.2005.

Поступила 23.11.09

УДК 003.26:004.056.55 **Климентов В.В., Трощило А.С.**

КРИПТОСИСТЕМА С «ВИРТУАЛЬНЫМ КЛЮЧОМ»

Возникновение и развитие области защиты информации (ЗИ) как неотъемлемой части информационной индустрии связано с острой необходимостью в средствах противодействия высокой уязвимости информационных технологий к различным злоумышленным действиям.

Совершенно очевиден тот факт, что информация по характеру не материальна, однако она всегда имеет стоимость, т.е. материальный эквивалент. Это свойство делает ее объектом копирования, модифицирования и хищения. Типичной является ситуация, когда совместное владение информацией наносит непоправимый ущерб одной из сторон, владеющей ею. Поэтому функция ЗИ актуальна практически во всех сферах коммуникации.

Постоянный рост и разнообразие задач, относящихся к сфере ЗИ, обусловлены тем, что информационные взаимодействия, развиваясь, приобретают все более сложный характер, соответственно становятся более разнообразными и изощренными угрозы в их сторону, а это, в свою очередь, приводит к возникновению новых задач.

Если раньше все потребности в защите информации сводились к обеспечению секретности и подлинности передаваемых сообщений, то есть к их защите от прочтения и внесения изменений, то сейчас количество проблем многократно возросло.

Особенно остро встала проблема защиты компьютерных сетей. Актуальность этой проблемы подтверждается следующими фактами.

США уже финансирует создание модели интернета будущего, где в условиях строгой секретности изучаются способы хакерского блокирования электросетей, сетей связи и аэропортов, а также финансовых рынков, дабы усовершенствовать как методы защиты, так и виртуальное оружие нового поколения.

На сегодняшний день в США возникла необходимость в создании «цифровых войск», которые смогли бы защитить страну от внешних электронных угроз, сообщает источник BBC. Идею создания подобного подразделения, которое бы занималось проблемами цифровой безопасности, озвучил глава АНБ США. Ожидается, что организация этого подразделения будет полностью завершена в 2010 г.