Таким образом, разработана теоретическая концепция позволяющая призводить идентификацию подлинности сигналограм на основе анализа фрактальных структур, присутствующих в них. В качестве дальнейших исследований необходимо изучения особенностей выявленных закономерностей в оценке подлинности цифрового сигнала.

Список литературы

10. *Рыбальский О.В.* К вопросу о фрактальности аналоговых сигналов, подвергнутых цифровой обработке // Вісник Східноукраїнського національного університету ім В. Даля. – Луганськ, 2006, № 9, ч. 1. – С. 21–25.

11. Командина Т.В., Соловьев В.И. Идентификация звукового устройства по статистическим характеристикам звукового файла // Вісник Східноукраїнського національного університету ім. В. Даля. – Луганськ, № 6, ч.1, 2009. – С. 169 – 172.

12. *Кобозева А.А., Рыбальский О.В., Струк И.А., Трифонова Е.А* Комплексный подход к экспертизе подлинности материалов цифровой звукозаписи // Вісник Східноукраїнського національного університету ім. В. Даля. – Луганськ, № 6, ч.1, 2009. – С. 75 – 78.

Поступила 17.02.2010

УДК 003.26:004.056.55:621.39 **Корченко О.Г., Гнатюк С.О., Васько О.В., Козирев С.П.**

КВАНТОВО-КРИПТОГРАФІЧНА СИСТЕМА З БЕЗУМОВНОЮ СТІЙКІСТЮ

Вступ

На даному етапі розвитку інформаційного суспільства все гостріше постає питання захищеності інформаційних ресурсів. Інформаційна безпека є однією із ключових складових національної безпеки. Із розвитком інформаційних технологій невпинно розвиваються і методи захисту інформації, однак, ще стрімкіше розвиваються методи несанкціонованого доступу до інформації. Це одвічне протистояння продовжується вже багато сотень років і з подальшим розвитком науки й техніки ставатиме все гострішим. Не є секретом і те, що стійкість математичних алгоритмів шифрування інформації (таких як DES, AES, RSA) – це всього лише питання часу і, з винайденням квантового комп'ютера, дані алгоритми шифрування будуть неактуальними і неефективними [1]. Отже, можна зробити припущення, що майбутнє криптографічної науки за квантовою криптографією. На даний момент відомо два основні напрямки квантової криптографії: квантовий прямий безпечний зв'язок (КПБЗ) та квантовий розподіл ключів (КРК) [2]. У протоколах КПБЗ легітимні користувачі (Аліса і Боб) взагалі не використовують шифрування, а передають інформацію шляхом кодування повідомлення за допомогою квантових станів фотонів. Протоколи КРК призначені для розподілу ключів шифрування між легітимними користувачами по квантовому каналу зв'язку.

Аналіз останніх досліджень

Проаналізувавши останні дослідження в даній галузі, можна зробити висновок про недосконалість і невисоку криптостійкість багатьох запропонованих систем. У більшості проаналізованих наукових публікацій [3-9] вирішується проблема розподілу ключів за допомогою систем КРК. Однак, будь-яка система шифрування з використанням КРК стійка на стільки, на скільки стійкий сам ключ. У статті [5] подано чіткий аналіз квантових технологій і методів захисту інформації, а також обумовлено переваги та недоліки кожного з квантових методів. У роботі [4] йдеться про те, що існує ще ряд невирішених проблем в

даній галузі (наприклад, вдосконалення алгоритмів виявлення підслуховування інформації в квантових каналах зв'язку). Для методу КРК були розроблені стеки протоколів [2], котрі включають: протокол первинної квантової передачі, протокол виправлення помилок, протокол для аналізу підслуховування і витоку інформації про ключ, протоколи підсилення секретності і формування кінцевого ключа У статті [6] було проведено аналіз надійності квантових протоколів розподілу ключів з використанням кубітів, а також багаторівневих квантових систем (кудитів). Крім того, існують реально діючі комерційні системи квантової криптографії [5], першою з яких була система QPN Security Gateway (QPN 8505) [7]. Дана система ефективно інтегрується в комп'ютерну мережу разом із традиційним мережевим обладнанням, включає в себе класичну технологію безпеки VPN та КРК. QPN 8505 є вигідним комерційним рішенням для урядових та фінансових організацій (генерує до ста 256 бітних ключів та працює на відстані до 140 км.). Система сумісна із такими протоколами як BB84, 3DES, AES. Однак, вартість даної системи на стільки висока, що для більшості потенційних клієнтів, зокрема у нашій країні, вона недоступна. Іншою прогресивною квантовою системою захисту інформації є Clavis id3000, яка розроблена компанію ID Quantique [8]. Clavis id3000 складається із двох станцій, які контролюються одним або двома зовнішніми комп'ютерами. Система призначена для передачі ключів на відстані до 100 км (на базі протоколів BB84 та SARG). Включає протокол формування кінцевого ключа та C++ бібліотеки для системного програмування. ID Quantique також пропонує систему під назвою Cerberis [5], що являє собою сервер з автоматичним створенням та секретним обміном ключами через захищений оптоволоконний канал (FC-1G, FC-2G, FC-4G). Дана система може передавати ключі на відстань до 50 км. Її характерною особливістю є 12 паралельних криптографічних обчислень, що значно підвищує швидкодію. Система використовує для шифрування AES (256 біт), а для розподілу ключів протоколи BB84 та SARG.

Проаналізувавши вищенаведені системи КРК, можна зробити висновок, що основним їхнім недоліком є використання математичних методів шифрування інформації (AES, 3DES, RSA). Стійкість цих методів вже зараз ставиться під сумнів, і зовсім скоро може скластися така ситуація, коли дані методи стануть неефективними для задач захисту інформації. У першу чергу, це може статися завдяки створенню квантового комп'ютера [1], для якого зламати стійкий математичний шифр буде справою кількох годин, а можливо і хвилин.

Основною метою роботи є підвищення рівня конфіденційності інформаційних ресурсів за рахунок створення моделі системи шифрування з теоретико-інформаційною стійкістю. Абсолютна стійкість системи буде забезпечена відповідною абсолютною стійкістю її базових компонентів (підсистеми розподілу ключів та підсистеми шифрування).

Основна частина

Для створення підсистеми розподілу ключів пропонується застосувати метод КРК (за протоколом BB84), а підсистема шифрування базуватиметься на методі одноразового блокноту Вернама [10]. У загальному вигляді квантова криптографія ґрунтується на основних принципах квантової механіки [2, 11]. Технологія квантової криптографії опирається на принципову невизначеність поведінки квантової системи – неможливо одночасно отримати координати і імпульс квантової частинки, тобто неможливо визначити один параметр фотона, не змінивши інший (принцип невизначеності Гейзенберга). Також, неможливо надійно розрізнити два неортогональних квантових стани, існує заборона на клонування [12], тобто неможливо створити точну копію невідомого квантового стану не впливаючи на початковий стан, наявність переплутаних квантових станів. Дві квантово-механічні системи можуть знаходитися у стані взаємної кореляції, а це, в свою чергу, означає, що вимірювання параметрів однієї з двох систем може рівноймовірно дати в результаті як $|0\rangle$, так і $|1\rangle$ (в той час як стан іншої системи буде протилежним і навпаки).

Квантова підсистема (підсистема розподілу ключів генерує і передає послідовності випадково поляризованих фотонів, які використовуються для формування ключа для подальшого шифрування (дешифрування) інформації. Це відбувається шляхом управління чотирма станами поляризації фотонів, які представляють два взаємопов'язаних ортогональних базиси *A* і *B*:

$$|0_A\rangle, |1_A\rangle, |0_B\rangle = \left(\frac{1}{\sqrt{2}}\right) \Big/ \left(|0_A\rangle + |1_A\rangle\right), |1_B\rangle = \left(\frac{1}{\sqrt{2}}\right) \Big/ \left(|0_A\rangle - |1_A\rangle\right) \quad (1)$$

Тут стани $|0_A>$, $|1_A>$ використовуються для кодування *«0»* і *«1»* в базисі *A*, а $|0_B>$, $|1_B>$ у базисі *B*. Дані стани можна визначити за допомогою поляризаційних станів фотонів. У протоколі BB84 носіями інформації є фотони, поляризовані під кутами 0^0, 45^0, 90^0, 135^0. Відповідно до законів квантової фізики [2, 11], за допомогою вимірювання можна розрізнити два лише ортогональних стани, тобто якщо відомо, що фотон поляризований горизонтально або вертикально, то за допомогою вимірювань можна визначити як саме. Те ж саме можна сказати і відносно поляризації в діагональному базисі. Однак, немає можливості достовірно відрізнити фотон поляризований під кутом 90^0, від того, який поляризований під кутом 45^0.

Відповідно до протоколу BB84, Аліса відправляє кубіт Бобу в одному з чотирьох поляризованих станів (0^0, 45^0, 90^0, 135^0). Боб, для того щоб розрізнити сигнали, володіє двома аналізаторами, один з яких розпізнає прямокутні базиси (вертикальну і горизонтальну поляризацію), інший – діагональні. Для того щоб відрізнити *«0»* від *«1»* Боб користується приладом (апаратом Штерна-Герлаха для електронів або поляризованими фотороздільником для фотонів) [13], який описується за допомогою двох ортогональних проекційних операторів $P_0=|0><0|$ та $P_1=|1><1|$. По відкритому каналу Боб повідомляє Алісі, які аналізатори були використані ним, у відповідь Аліса повідомляє Бобу, які аналізатори він вибрав правильно. Ті біти, для яких були вибрані правильні аналізатори, формують ключ, інші – відкидаються.

Припустимо, в каналі присутній зловмисник (по традиції назвемо його Євою), і він володіє таким самим обладнанням як Боб. Найбільш доцільним для Єви є метод заміни. Для цього Єва аналогічно Бобу приймає фотони, занотовує базиси та результати вимірювання, далі вона передає сигнал у тому базисі, в якому він був прийнятий. Як згадувалося раніше, Єва не може виміряти характеристику фотона, не змінивши його стан, не може здійснити вимірювання над кубітом у двох різних базисах, а також не може зробити копію стану кубіту і дочекатися поки Аліса та Боб оголосять базиси. Зрозуміло, що приблизно у 50% випадків Єва не правильно вибере базис, а, отже, отримає не вірне значення кубіту. Потім вона створить новий фотон, поляризований у випадковому базисі, і відправить його Бобу. Через неправильний вибір базису Євою результати вимірювань Боба будуть відрізнятися від результатів Аліси приблизно на 25%. Цей тип атаки називають некогерентною або індивідуальною (Єва опрацьовує кожен фотон Аліси окремо) та непрозорою (Єва не пропускає фотони Аліси по каналу, а випромінює їх заново). Детальний аналіз різних типів атак, а також аналіз надійності протоколу BB84 наведено у статті [6]. Після закінчення передачі по квантовому каналу Аліса та Боб встановлюють зв'язок через відкритий канал для узгодження базисів і з'ясування, які із бітів будуть надалі використовуватися в ключі. При цьому йде розголошення базисів, а не самих результатів вимірювання. Після чого проводиться аналіз кількості помилок для виявлення втручання Єви. Також для підвищення достовірності виявлення зловмисника може бути відкрито разом з базисами частину бітів ключа (які надалі будуть відкинуті). Дана процедура підсилення секретності добре описана в роботі [3]. Зауважимо, що дані методи виявлення зловмисника дійсно ефективні при однофотонній передачі інформації в квантовому каналі.

Підсистема шифрування

Протокол ВВ84 забезпечує розподіл ключів, які будуть використовуватися для криптографічних перетворень у підсистемі шифрування. Однак, зважаючи на те, що стійкість традиційних методів шифрування (AES, 3DES, RSA та ін.) не є абсолютною, пропонується метод шифрування з теоретико-інформаційною (безумовною, абсолютною) стійкістю. Такою властивістю володіє метод одноразового блокноту Вернама [10]. Даний метод розроблений в 1917 році Джозефом Моборном і Гільбертом Вернамом. У класичному варіанті одноразовий блокнот – це велика неповторна послідовність символів ключа, розподілених випадковим чином. Спочатку це була одноразова стрічка для телетайпів. Відправник використовував один символ ключа для шифрування одного символу відкритого тексту. При цьому використовувалися дві однакові стрічки, перша з яких знаходилася у відправника, інша – у приймача. Коли відправник збирався відправити повідомлення, він спочатку перетворював його у двійковий вигляд. Потім стрічка з двійковим кодом розміщувалася у спеціальному апараті, котрий додавав за модулем два до бітів початкового повідомлення кожен біт ключа відповідно. На приймаючій стороні здійснювалась та ж сама операція, тобто відбувалась взаємна компенсація ключів. Даний метод доцільно використовувати для шифрування інформації, яка зберігається у двійковому вигляді чи передається по комп'ютерній мережі. Відмінність у тому, що операція «виключне або» між відкритим текстом та ключем буде здійснюватися в електронному вигляді. Для забезпечення абсолютної криптографічної стійкості ключ повинен володіти наступними властивостями: бути істинно випадковим; бути не меншим за розміром, ніж початкове повідомлення; має застосовуватися тільки один раз (бути одноразовим).

У 1949 році Клод Шеннон опублікував відому роботу [14], в якій довів абсолютну стійкість шифру Вернама. Це по суті означає, що шифр Вернама є найбільш безпечною криптосистемою із усіх існуючих. Однак, при цьому умови, яким повинен відповідати ключ, на стільки складні, що практичне використання даного шифру стає важко здійсненним. Зважаючи на це, одноразовий блокнот використовується тільки для передачі повідомлень найвищої секретності. Таким чином, пропонується стек протоколів, відповідно до якого ключі будуть розподілятися вищезгаданим квантовим методом (ВВ84), а шифрування здійснюватиметься методом одноразового блокноту. На рис.1 зображено узагальнений стек протоколів з використанням протоколу ВВ84 та кодування за методом Вернама.

Даний стек протоколів відображає порядок здійснення процедури передачі ключа по квантовому каналу з подальшим шифруванням повідомлення цим ключем. Наведемо приклад практичної реалізації запропонованого стеку протоколів. Припустимо, перед нами стоїть завдання зашифрувати повідомлення «cryptography» (слід звернути увагу на регістр букв, тому що в таблиці ASCII літери верхнього і нижнього регістру мають різні значення кодів). У табл.1 приведено витяг кодів з ASCII-таблиці для літер, що зустрічаються у повідомленні. Коди подані в десятковій та двійковій формах.

Враховуючи те, що кожна літера кодується за допомогою восьмибітного числа, довжина повідомлення складатиме 96 біт, і відповідно довжина ключа повинна бути такою ж (не меншою). Аліса випадковим чином генерує ключ і за допомогою спеціального пристрою посилає його Бобу у вигляді слабких імпульсів поляризованого світла. Поляризація керується за допомогою комірки Поккельса, що дає можливість Алісі вибрати між чотирма варіантами (0^0, 45^0, 90^0, 135^0). На стороні Боба ще одна комірка Поккельса контролює поворот схеми: 0^0 відповідає вимірюванню у прямокутному базисі, 45^0 – в діагональному. Поляризаційний світлороздільник розділяє промінь на два ортогональні компоненти, котрі уловлюються одним із двох діодів (відповідно до використаних діодів у результаті буде *«0»* або *«1»*).

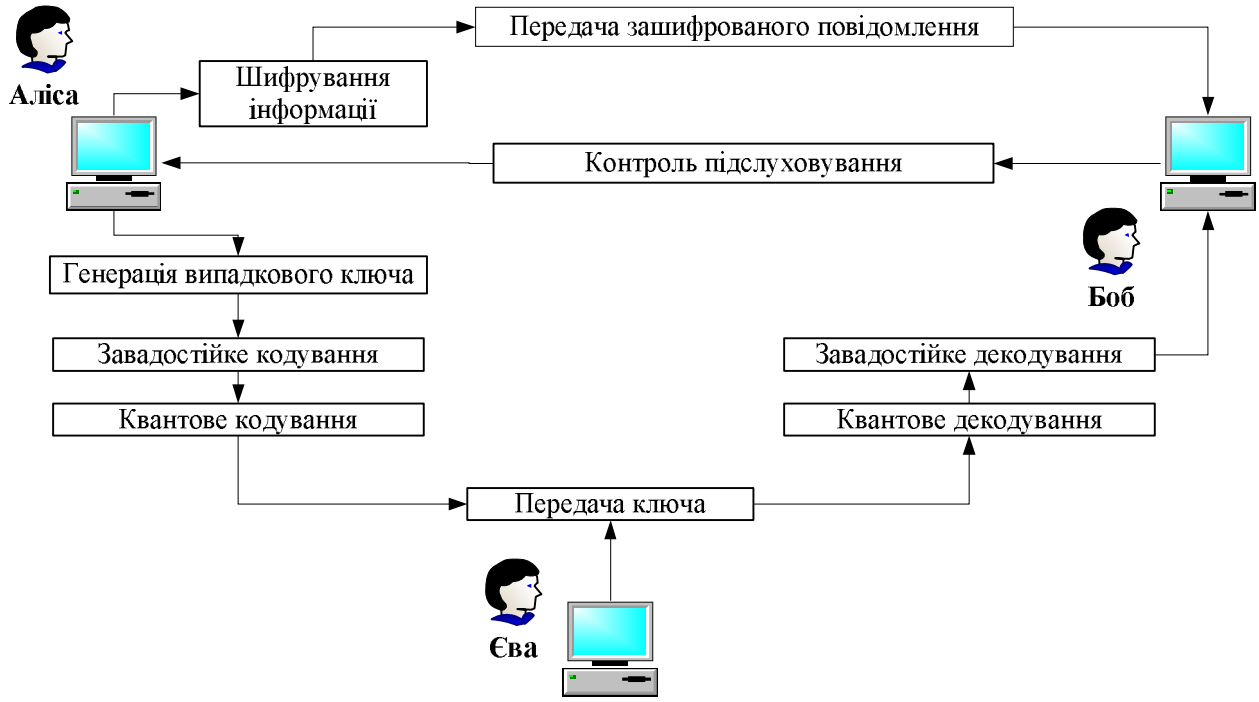

Рис.1 Узагальнений стек протоколів квантово-криптографічної системи з безумовною стійкістю

Враховуючи те, що при аналізі отриманих фотонів приблизно у 50% випадків, Боб неправильно обере базис, довжину ключа, який генерує Аліса, потрібно збільшити як мінімум удвоє. Вважатимемо, що Аліса і Боб використовують ідеальний канал зв'язку, так як в іншому разі слід врахувати також відсоток викривлень, спричинених завадами у каналі зв'язку. Для того щоб передати повідомлення розміром 96 біт Аліса генерує 200 бітний ключ.

Таблиця 1
Кодування повідомлення

№	Літера	Десятковий код	Двійковий код	№	Літера	Десятковий код	Двійковий код
1	c	99	01100011	7	g	103	01100111
2	r	114	01110010	8	r	114	01110010
3	y	121	01111001	9	a	97	01100001
4	p	112	01110000	10	p	112	01110000
5	t	116	01110100	11	h	104	01101000
6	o	111	01101111	12	y	121	01111000

Приклад процесу генерації ключа показано у табл. 2:

Таблиця 2
Алгоритм генерації ключа

Послідовність фотонів Аліси	|	–	/	|	/	–	/	….	/	–	\	|	|	–	–
Послідовність аналізаторів Боба	+	+	x	x	+	+	x	….	+	+	x	x	x	+	x
Результати вимірювань Боба	0	1	0	1	0	1	0	….	1	1	1	0	1	1	0
Аналізатори, які вибрані вірно	+	+	+			+	+	….		+	+			+	
Ключ	0	1	0			1	0	….		1	1			1	

Отже, відбувається генерація ключа і його передача по квантовому каналу зв'язку. Доцільним є також завадостійке кодування, наприклад, за допомогою коду Хемінга [15].

Після того як Боб прийняв ключ відбувається узгодження базисів. Воно продовжується до тих пір, поки не буде з'ясовано, що Боб розпізнав правильно ту кількість кубітів, яка необхідна для кодування повідомлення (у даному випадку 96 кубітів). Після цього, Аліса шифрує повідомлення за вищевикладеним принципом. Початкове повідомлення у двійковому виді має вигляд:

01100011 01110010 01111001 01110000 01110100 01101111

01100111 01110010 01100001 01110000 01101000 01111000

Припустимо ключ, згенерований Алісою – наступна послідовність:

01010110 00110100 00110110 01110110 00101110 01000101

10111011 01101010 11111111 01011000 01101100 01000111

Після виконання операції шифрування повідомлення прийме вигляд:

00110101 01000110 01001111 00000110 01011010 00101010

11011100 00011000 10011110 00101000 00000100 00111111

Якщо Єва перехопить дане повідомлення під час передачі по відкритому каналу, не маючи ключа, і спробує його розшифрувати за допомогою ASCII-таблиці (чи інших засобів) то отримає набір абсолютно безкорисних символів.

Висновки

Таким чином, у даній роботі запропонована модель квантово-криптографічної системи з використанням квантового розподілу ключів за протоколом BB84 та шифрування методом Вернама. Основною перевагою даної системи є теоретико-інформаційна стійкість, що забезпечується відповідною теоретико-інформаційною стійкістю вищезгаданих підсистем розподілу ключів і системи шифрування Вернама.

Однак дана система має ряд недоліків, таких як наприклад складність практичної реалізації. Як згадувалося раніше, довжина ключа повинна бути такою ж як і довжина самого повідомлення. Для передачі такого ключа необхідний квантовий канал з досить високою пропускною здатністю, що поки є проблемою для існуючих систем КРК. Інша проблема – складність програмної реалізації системи шифрування Вернама, що в першу чергу стосується рандомізації елементів ключа. Іншими словами – необхідність забезпечення реальної випадковості, а не псевдовипадковості ключа, що можна забезпечити лише при використанні хаотичних фізичних процесів (наприклад, білий шум, броунівський рух молекул). У якості підсилення запропонованої системи можна додатково використати шифрування асиметричними методами у відкритому каналі, по якому здійснюється узгодження базисів. У випадку спроби перехоплення ключа Євою такий захист не дасть їй можливості доступу до базисів, які використовувалися Алісою при кодуванні ключа.

Виконана робота залишає широке поле для подальших фундаментальних досліджень у даному напрямі. Як альтернативу можна розглядати використання у підсистемі шифрування протоколів квантового потокового шифру (наприклад, Y-00), що передбачає шифрування даних подібно до класичних потокових шифрів (але із застосуванням квантового шумового ефекту). Теоретико-інформаційна стійкість протоколу Y-00 забезпечується рандомізацією, що базується на квантовому шумі, а також на додаткових складних математичних схемах. Чи не єдиною проблемою на сьогодні залишається складність практичної реалізації даного методу.

Список літератури

1. *Валиев К.А.* Квантовая информатика: компьютеры, связь и криптография / Валиев К.А. // Вестник РАН. – Том 70. – № 8, 2000. – С. 688–695.
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. *Слепов Н.* Квантовая криптография: передача квантового ключа. Проблемы и решения // Электроника: НТБ. – 2006, №2. – С. 54–61.
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. *Корченко О.Г.* Сучасні квантові технології захисту інформації / *Корченко О.Г., Василіу Є.В., Гнатюк С.О.* // Захист інформації. – №1, 2010. – С. 77–89.
6. *Василиу Е.В.* О надежности квантовых протоколов распределения ключей. I Протоколы с передачей кубитов // Наукові праці ОНАЗ ім. О.С. Попова. – 2007, №1. – С. 5-17.
7. *MagiQ.* Products. QPN Security Gateway. [Електронний ресурс]. – Режим доступу: <http://www.magiqtech.com/MagiQ/Products.html>.
8. *ID* Quantique. Clavis id3000. [Електронний ресурс]. – Режим доступу: <http://www.idquantique.com/products/clavis id3000.html>.
9. *ID* Quantique. Cerberis. [Електронний ресурс]. – Режим доступу: <http://www.idquantique.com/products/cerberies.htm>.
10. *Синельников А.* Шифры советской разведки. [Електронний ресурс]. – Режим доступу: <http://hronos.km.ru/statii/2008/shifr5.html>
11. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – М. : Мир, 2006. – 824 с.
12. *Wooters W.K., Zurek W.H.* A single quantum cannot be cloned // Nature. – 1982. – V. 299. – P. 802.
13. *Гомонай О.В.* Лекції з квантової інформатики: Навчальний посібник. – Вінниця: О.Власюк, 2006. – С. 62–74.
14. *Shannon C.* Communication Theory of Secrecy Systems, Bell Systems Technical Journal, Vol. 28, pp. 656–715, 1949.
15. *David J.C. MacKay.* Information Theory, Interference and Learning Algorithms. – Cambridge: Cambridge University Press, 2003. – ISBN 0-521-64298-1.

Надійшла 16.03.2010

УДК 681.3 **Сірченко Г.А.**

ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ В КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Вступ

Задача забезпечення усіх основних функціональних властивостей захищених систем, в тому числі і цілісності та доступності їх інформаційних ресурсів, може вирішуватися як загальносистемними засобами технічного захисту інформації (ТЗІ), так і засобами, які є вбудованими в елементи таких автоматизованих систем (АС). При цьому можна і слід говорити про необхідність забезпечення цілісності та доступності ресурсів по відношенню до кожного з елементів АС, в тому числі по відношенню до телекомунікаційної мережі (ТКМ) АС, та застосування у складі цієї підсистеми певних методів, способів та засобів забезпечення захисту проти загроз цілісності та доступності інформаційних об'єктів.

Аналіз публікації

З матеріалів досліджень, викладених в [1,2,3] витікає, що до складу комунікаційної мережі (КМ) (і, відповідно, засобів захисту кожної з властивостей захищеності інформаційних ресурсів КМ входять засоби забезпечення обміну інформацією (елементи телекомунікаційної мережі) з їх засобами забезпечення відповідних властивостей захищеності в телекомунікаційних мережах КМ (і, зрозуміло, в засобах обміну інформацією локальних обчислювальних мереж, як елементів таких КМ). Це дозволяє сформулювати